DASC 45th
Digital Avionics Systems Conference
Orlando, Florida, USA - September 13-17, 2026

Runtime Safety Filtering for Learned Small UAS Separation Policies under GNSS Degradation

Action filtering vs observation filtering

Alex Zongo · Peng Wei

Department of Mechanical and Aerospace Engineering
George Washington University, Washington, DC, USA.

01 MOTIVATION

A learned separation policy can resolve conflicts

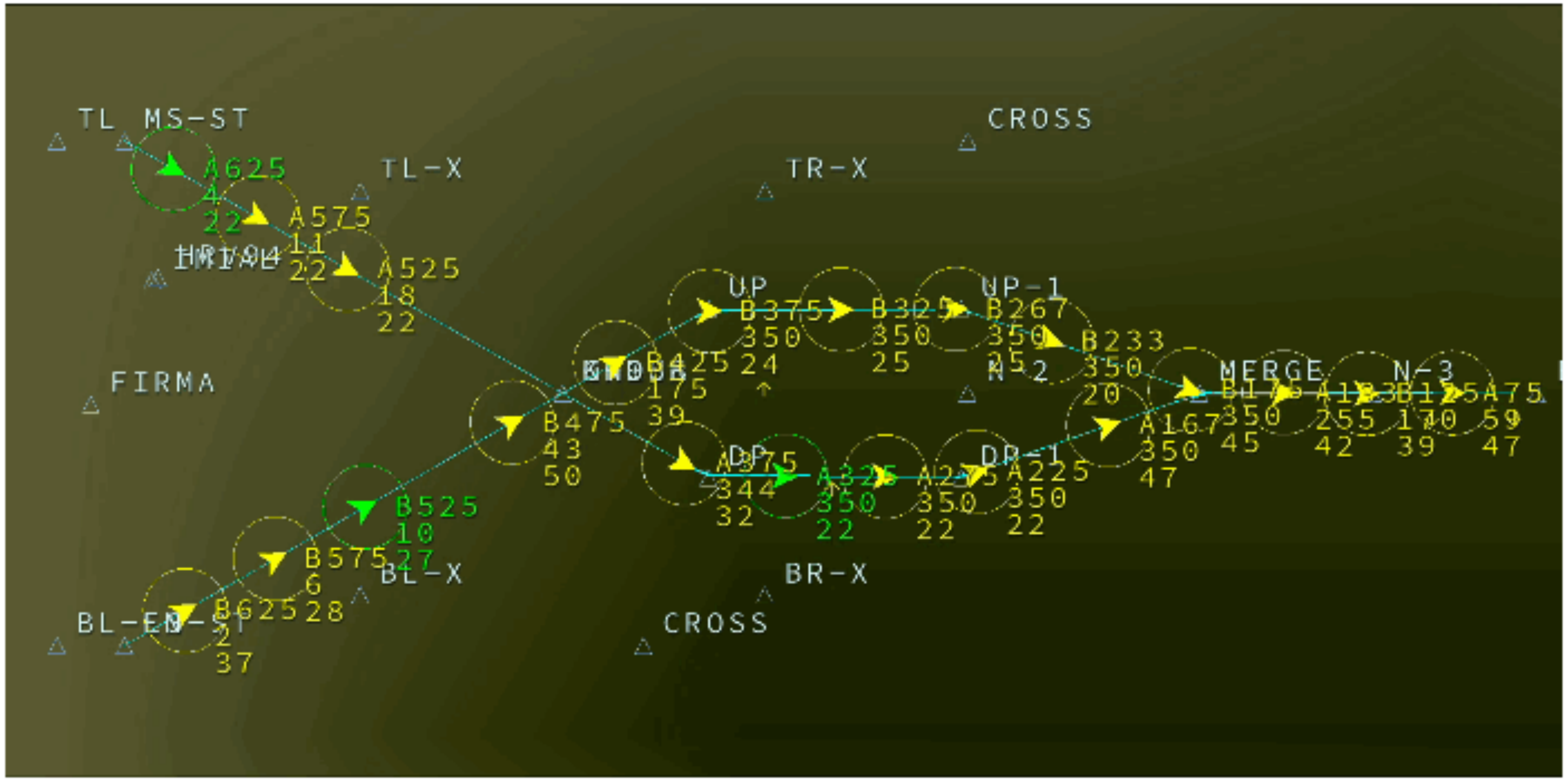
With nominal GNSS, the policy produces a separation-preserving action.

The policy uses nearby aircraft information to adjust ownship speed in real time.

100 m separation standard
10 km routes

Next: What information does the policy receive, and how can GNSS degradation corrupt it?

SIMULATION · NO GNSS DEGRADATION (NOMINAL GNSS)



A learned separation policy can resolve conflicts

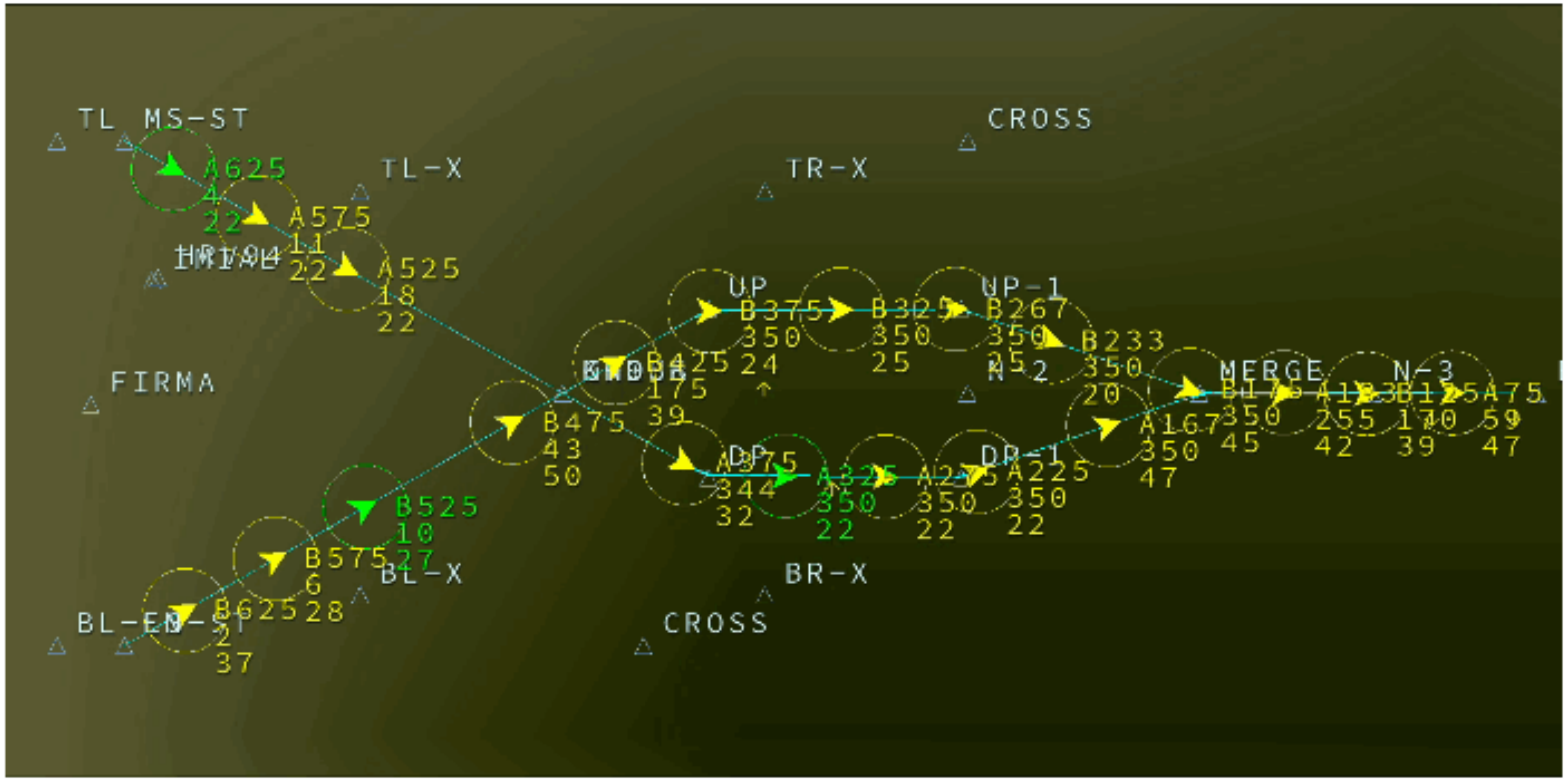
With nominal GNSS, the policy produces a separation-preserving action.

The policy uses nearby aircraft information to adjust ownship speed in real time.

100 m separation standard
10 km routes

Next: What information does the policy receive, and how can GNSS degradation corrupt it?

SIMULATION · NO GNSS DEGRADATION (NOMINAL GNSS)



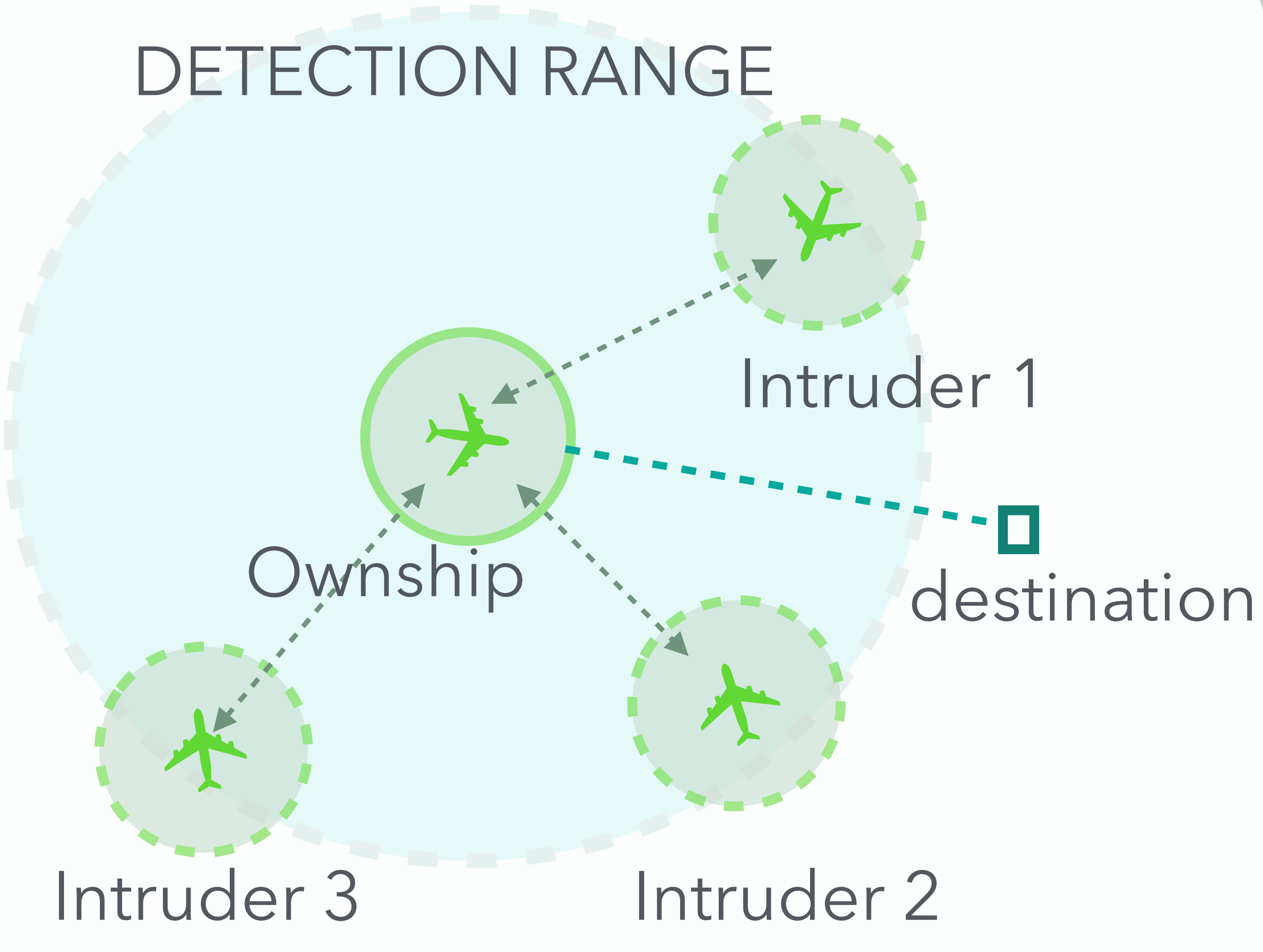
How a <u>decentralized</u> learned separation policy works

How a decentralized learned separation policy works

1. LOCAL TRAFFIC

How a decentralized learned separation policy works

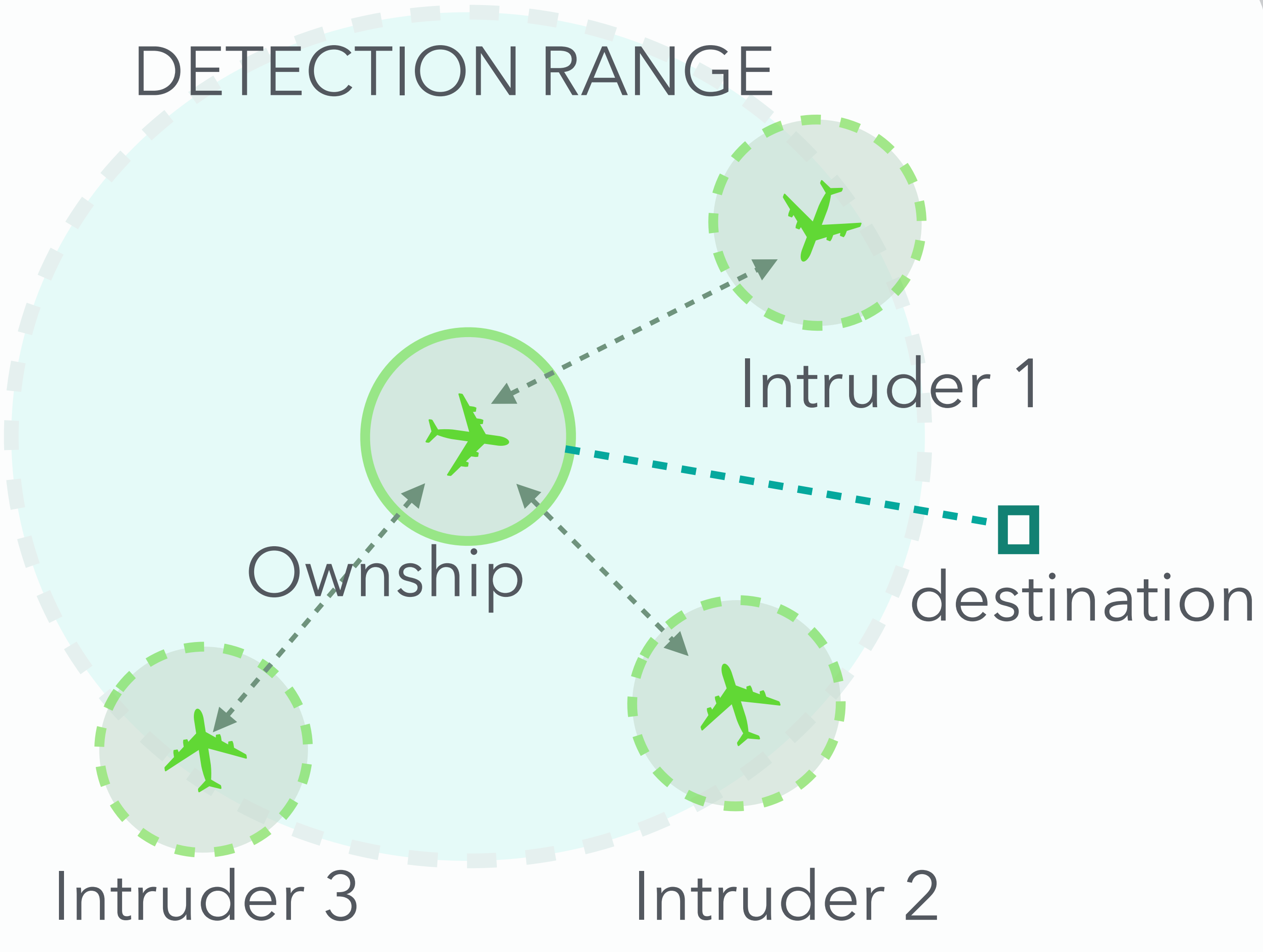
1. LOCAL TRAFFIC



Traffic within sensing range,
broadcast over Remote ID

How a decentralized learned separation policy works

1. LOCAL TRAFFIC

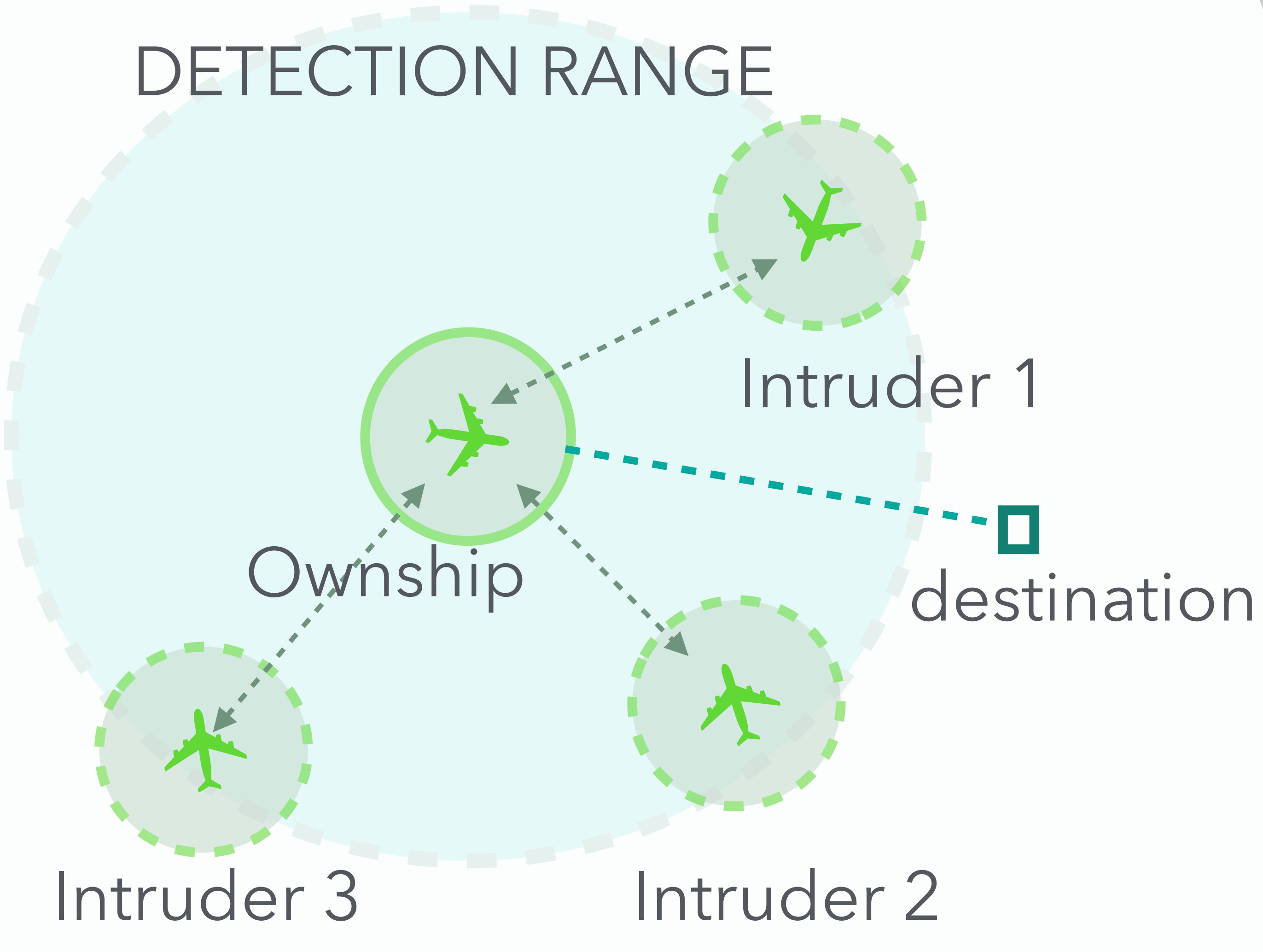


Traffic within sensing range, broadcast over Remote ID

2. LOCAL OBSERVATION

How a decentralized learned separation policy works

1. LOCAL TRAFFIC

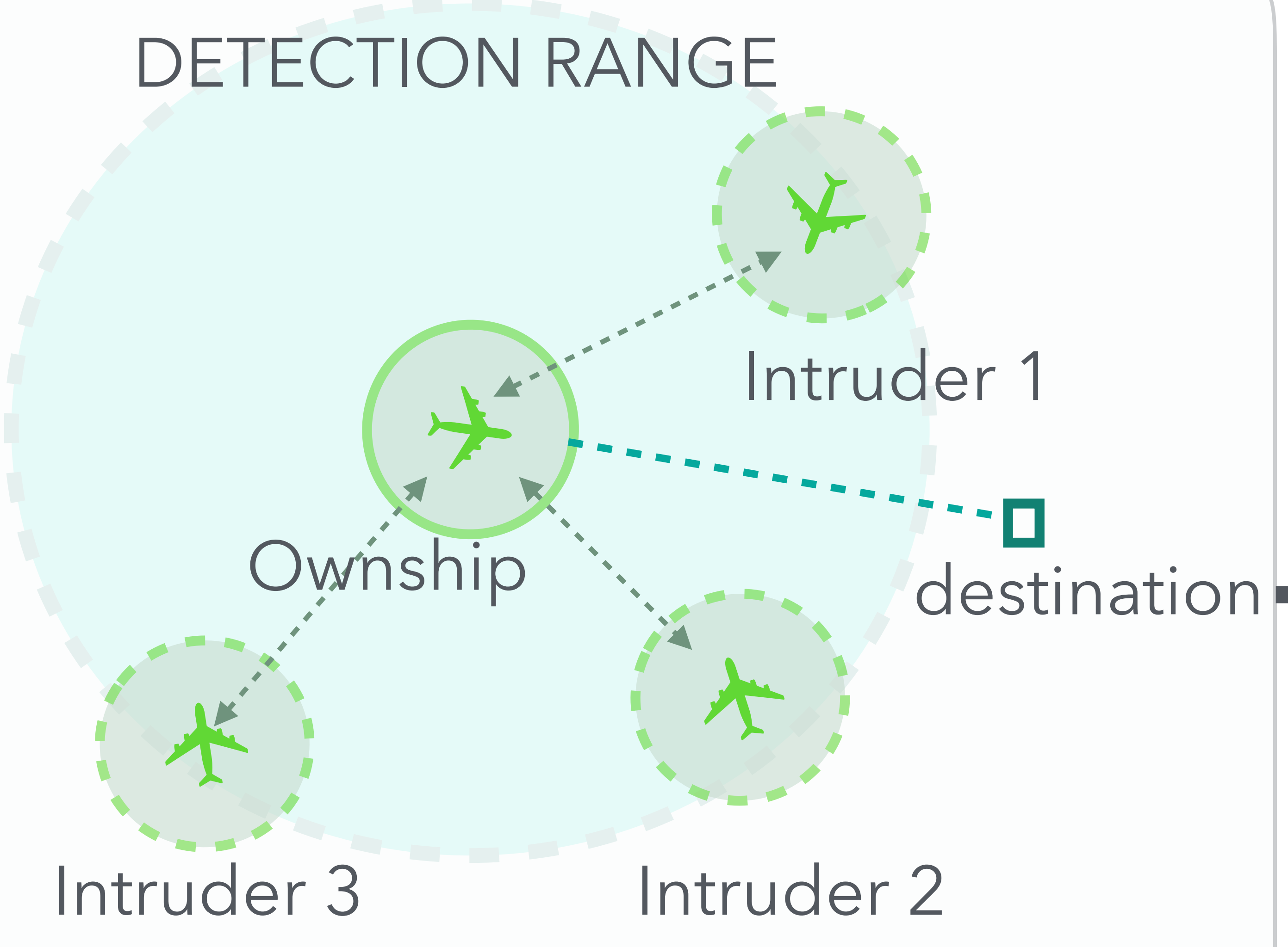


Traffic within sensing range, broadcast over Remote ID

2. LOCAL OBSERVATION

How a decentralized learned separation policy works

1. LOCAL TRAFFIC



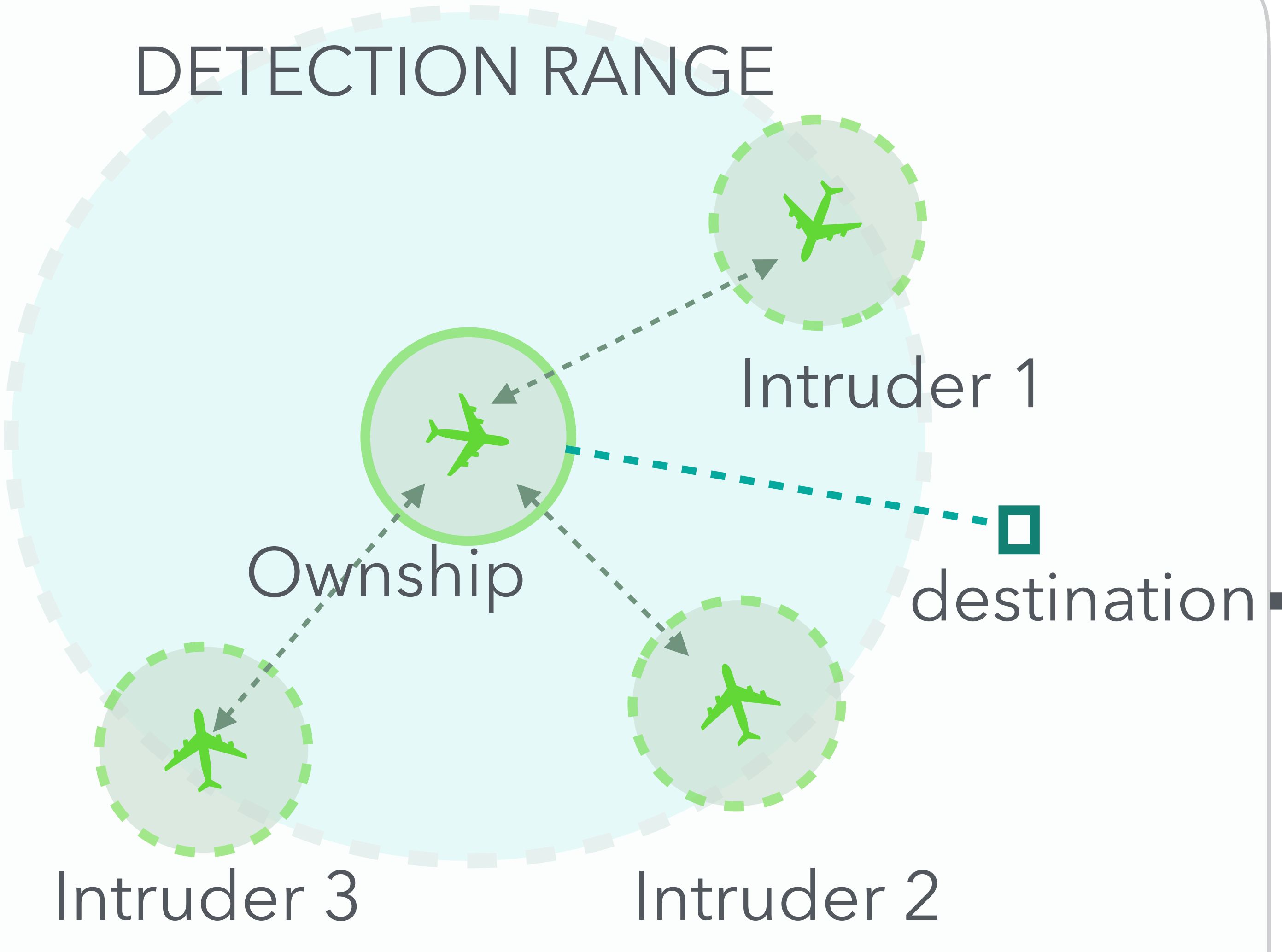
Traffic within sensing range,
broadcast over Remote ID

2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

How a decentralized learned separation policy works

1. LOCAL TRAFFIC



Traffic within sensing range,
broadcast over Remote ID

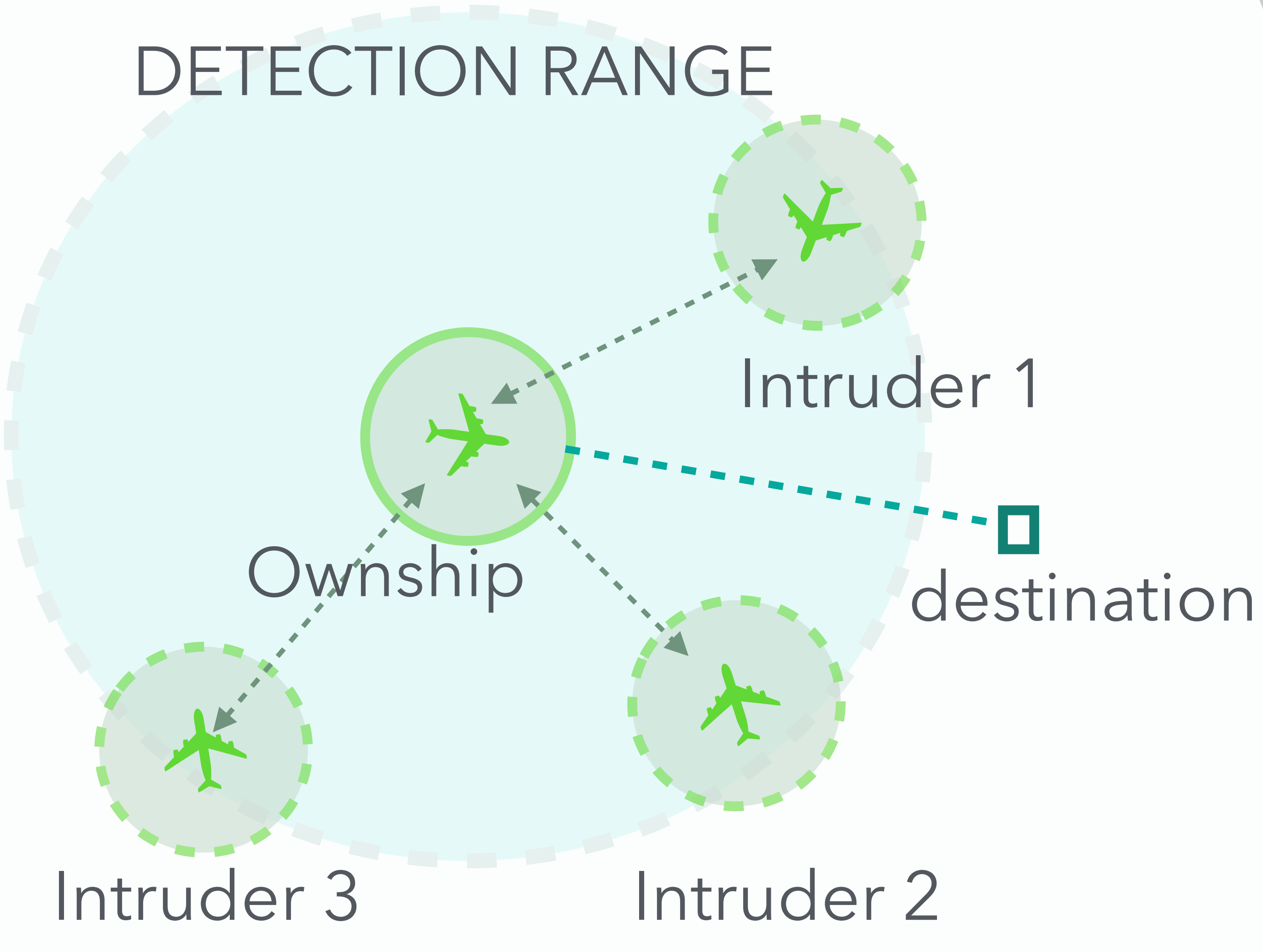
2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

3. POLICY TO ACTION

How a decentralized learned separation policy works

1. LOCAL TRAFFIC



Traffic within sensing range,
broadcast over Remote ID

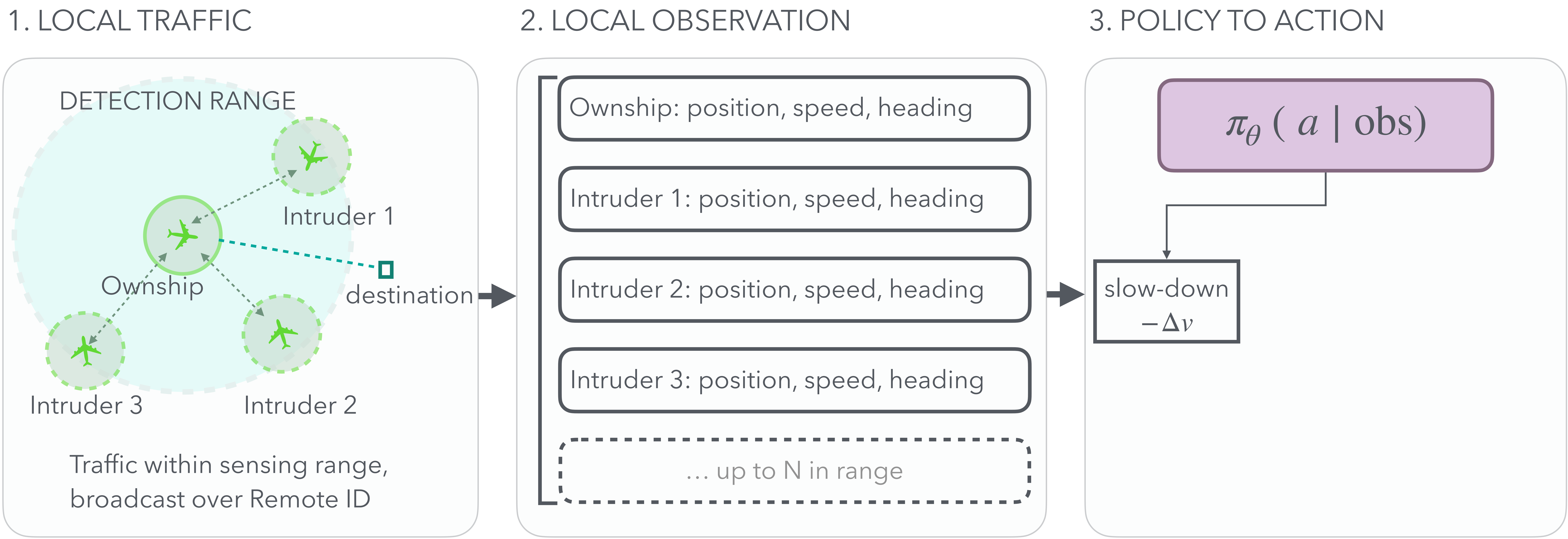
2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

3. POLICY TO ACTION

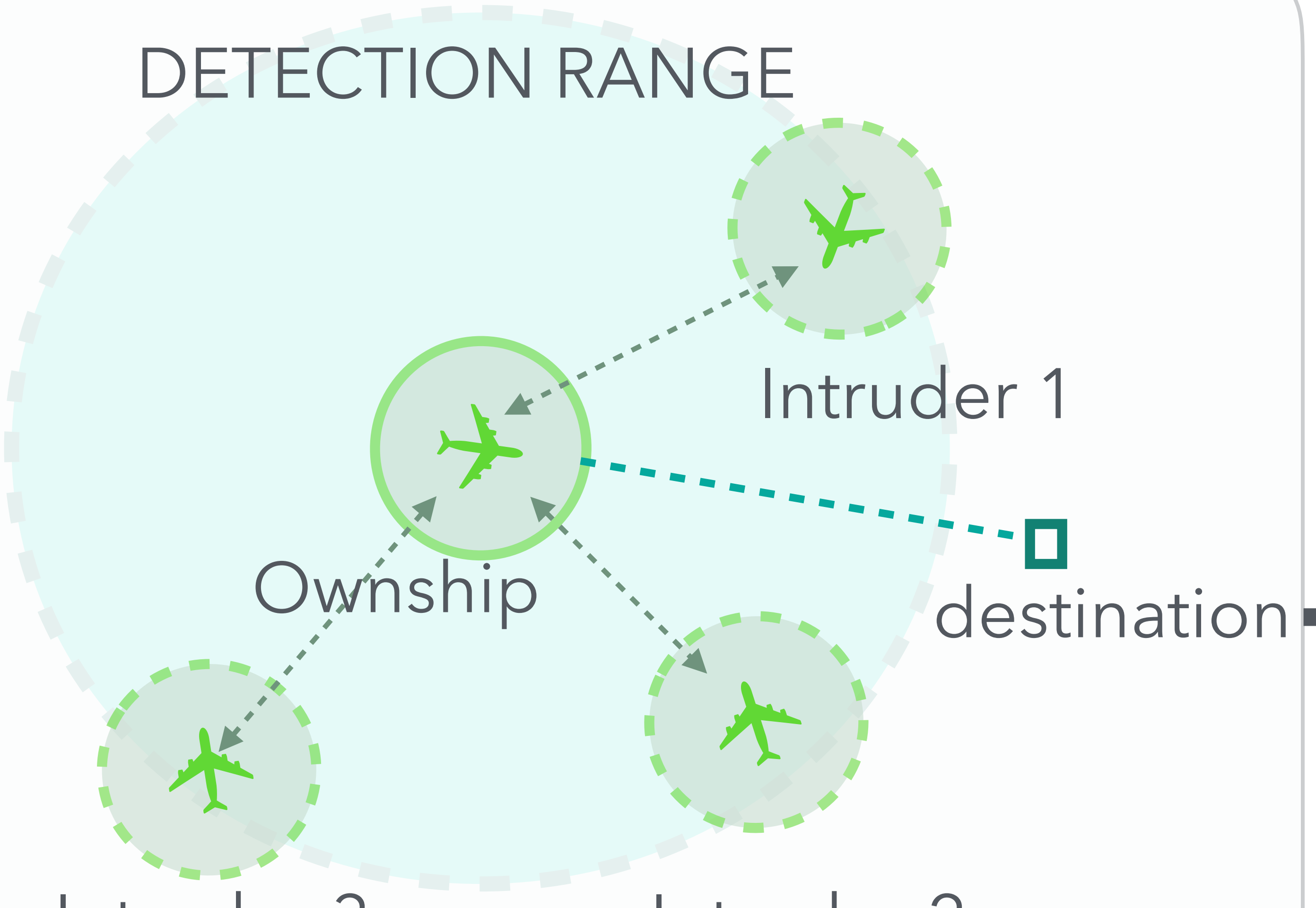
$$\pi_\theta\,(\,a \mid \mathrm{obs})$$

How a decentralized learned separation policy works



How a decentralized learned separation policy works

1. LOCAL TRAFFIC



Traffic within sensing range,
broadcast over Remote ID

2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

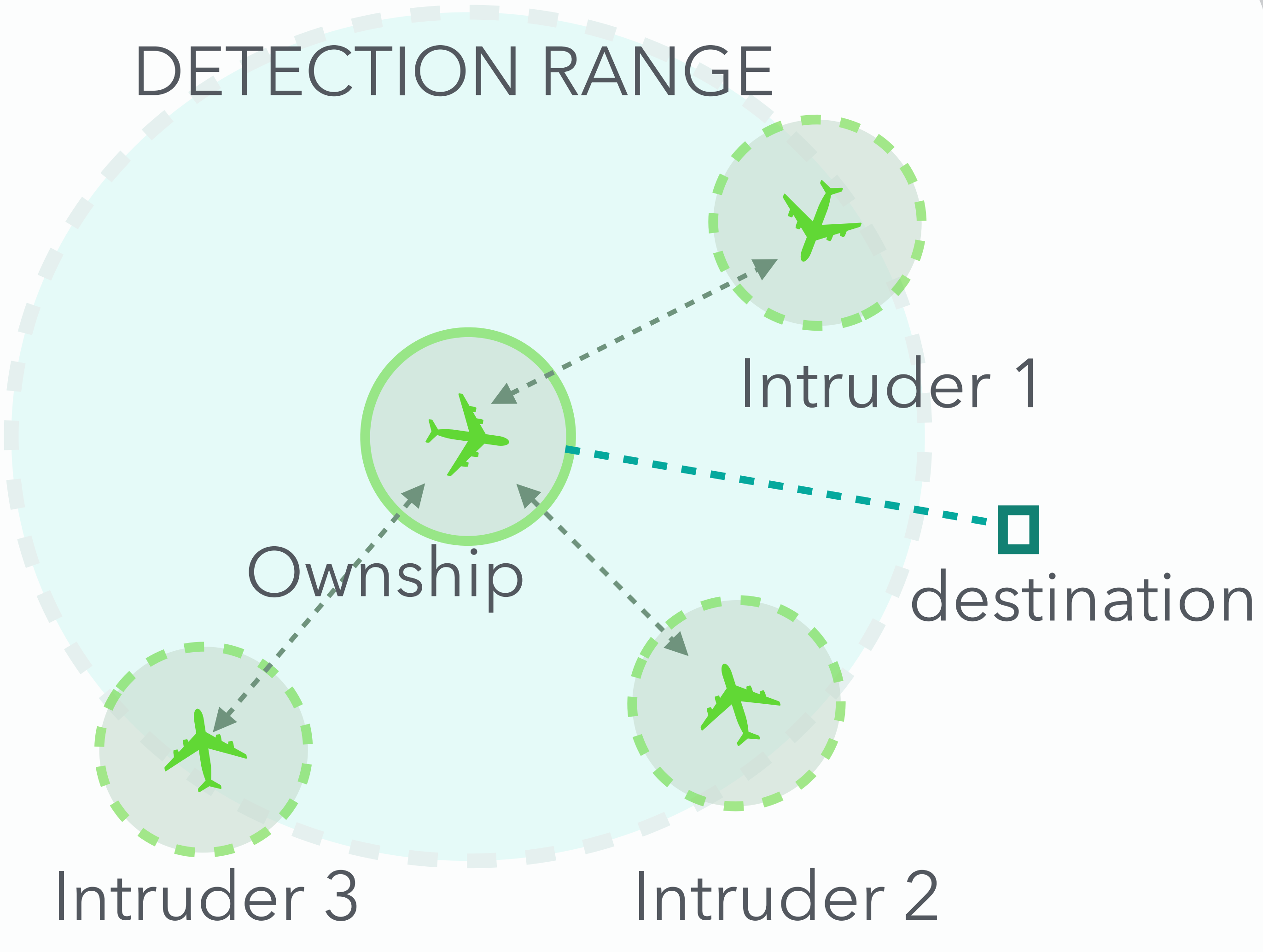
3. POLICY TO ACTION

$$\pi_\theta\,(\,a \mid \mathrm{obs})$$

slow-down $-\Delta v$	hold speed ± 0

How a decentralized learned separation policy works

1. LOCAL TRAFFIC



Traffic within sensing range,
broadcast over Remote ID

2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

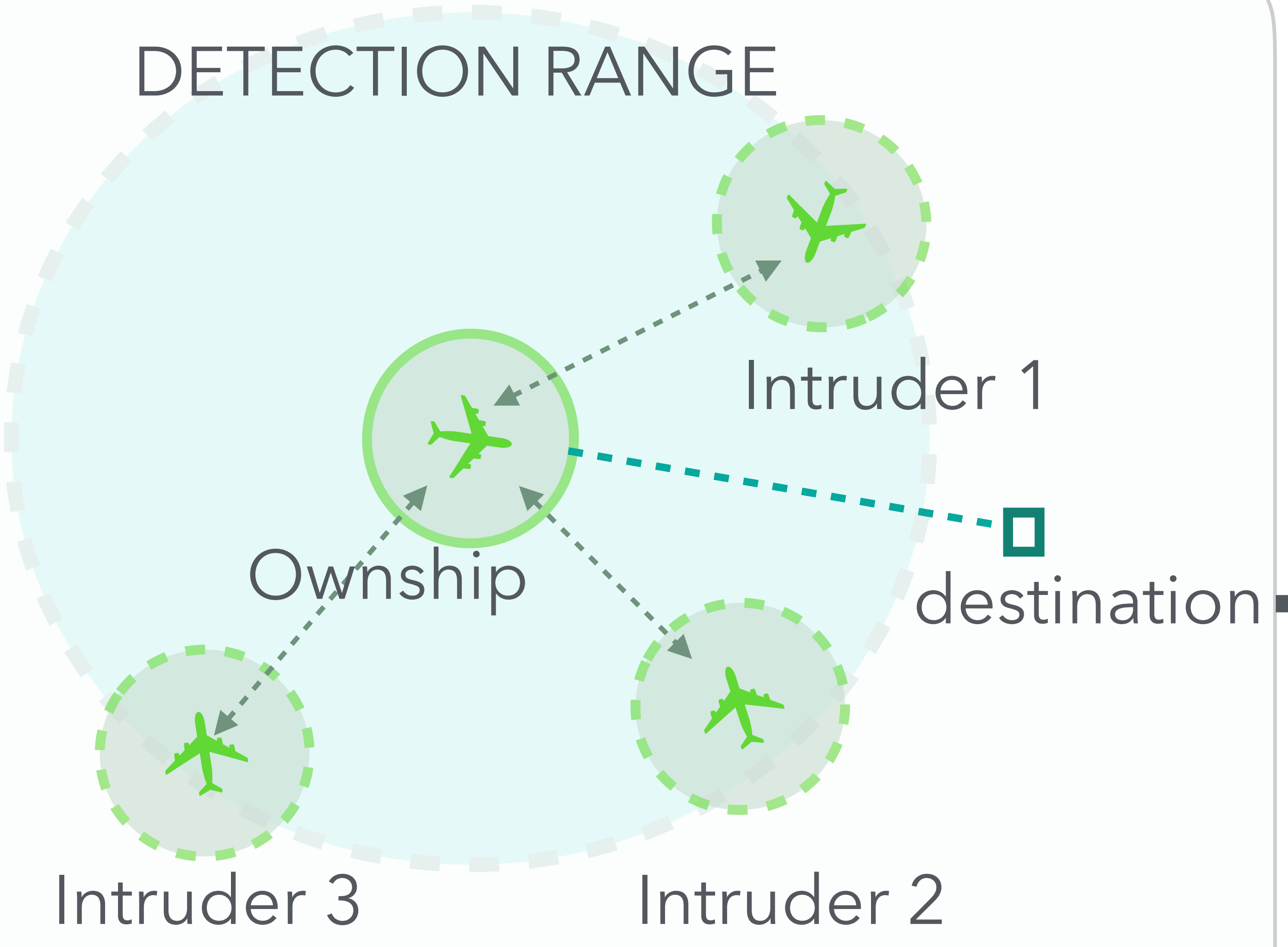
3. POLICY TO ACTION

$$\pi_\theta\,(\,a \mid \mathrm{obs})$$

slow-down	hold speed	speed up
$-\Delta v$	± 0	$+\Delta v$

How a <u>decentralized</u> learned separation policy works

1. LOCAL TRAFFIC



Traffic within sensing range, broadcast over Remote ID

2. LOCAL OBSERVATION

- Ownship: position, speed, heading
- Intruder 1: position, speed, heading
- Intruder 2: position, speed, heading
- Intruder 3: position, speed, heading
- … up to N in range

3. POLICY TO ACTION

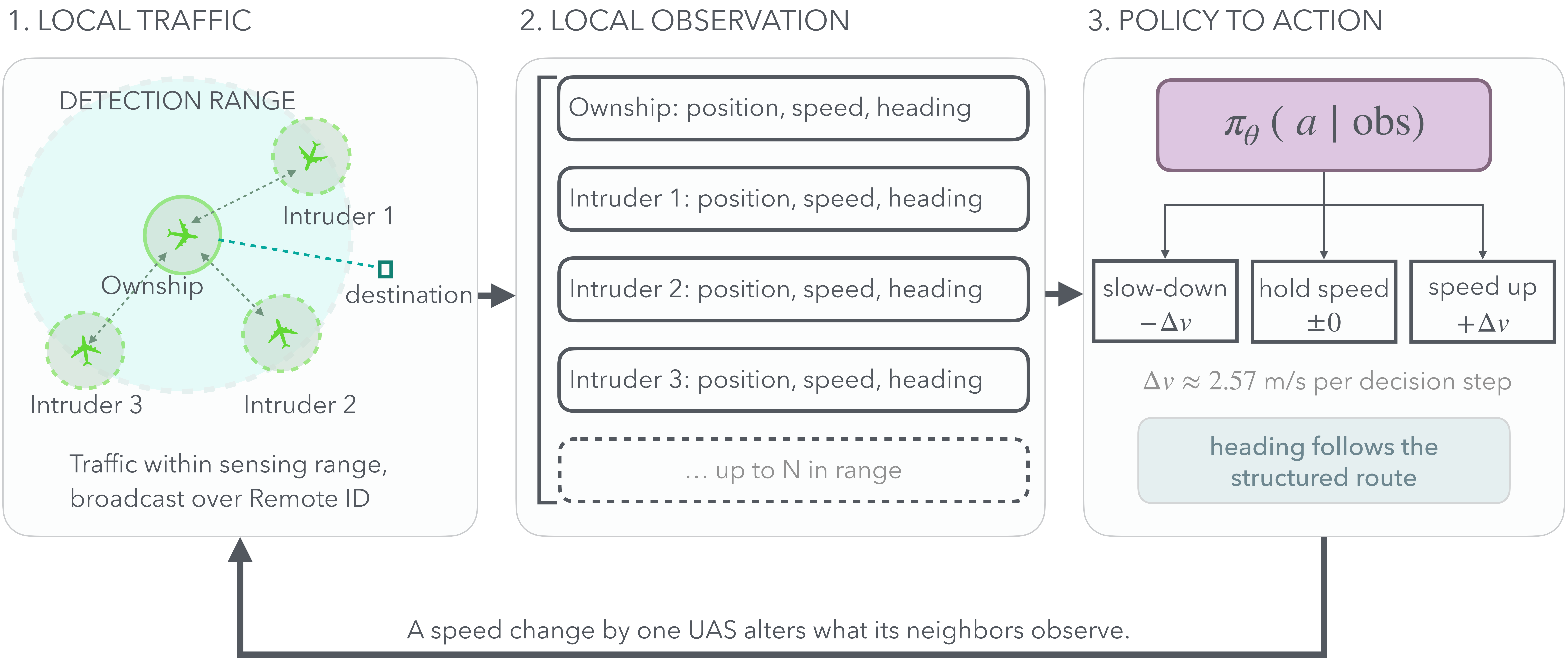
$\pi_\theta\ (\ a \mid \mathrm{obs})$

slow-down	hold speed	speed up
$-\Delta v$	± 0	$+\Delta v$

$\Delta v \approx 2.57$ m/s per decision step

heading follows the structured route

How a decentralized learned separation policy works



GNSS degradation distorts the state the policy relies on

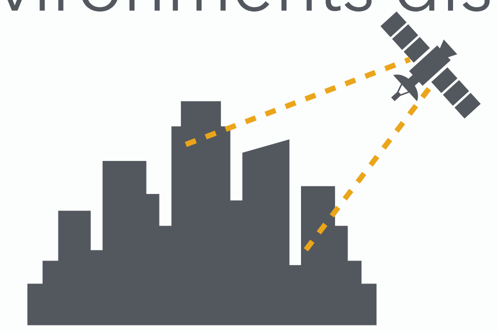
GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

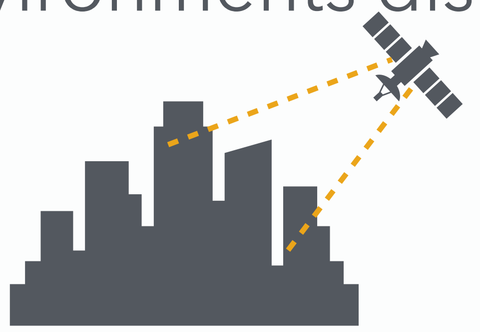
Urban environments disrupt navigation integrity

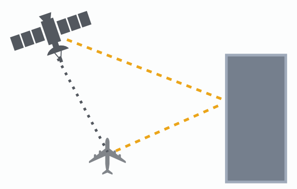


GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity





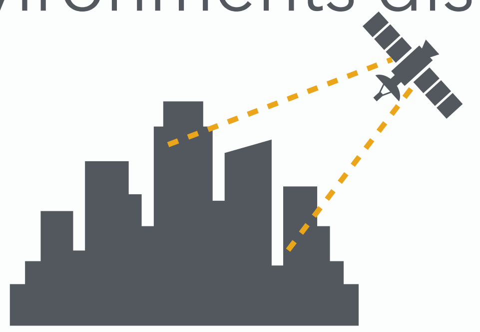
Multipath

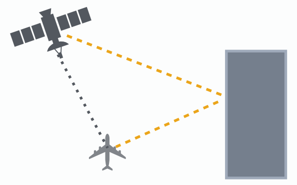
Reflections from building faces bias position estimation

GNSS degradation distorts the state the policy relies on

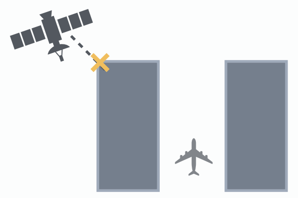
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity





Multipath
Reflections from building faces bias position estimation



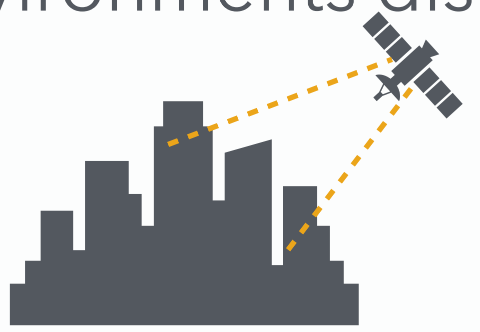
Blockage
Urban canyons create gaps and unstable fixes

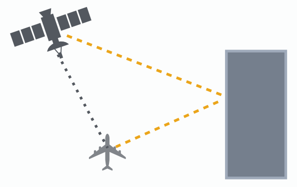
02 THE PROBLEM

GNSS degradation distorts the state the policy relies on

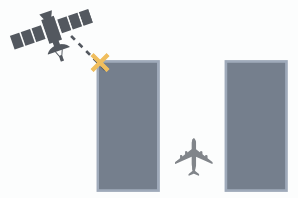
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

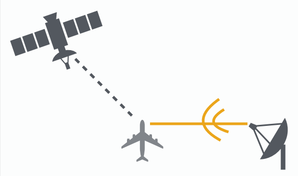




Multipath
Reflections from building faces bias position estimation



Blockage
Urban canyons create gaps and unstable fixes



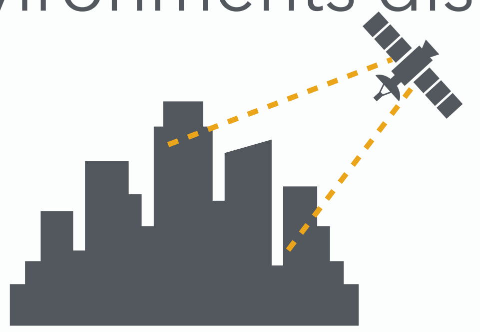
Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

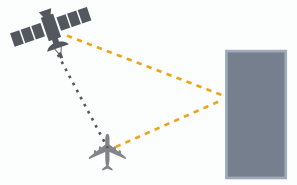
02 THE PROBLEM

GNSS degradation distorts the state the policy relies on

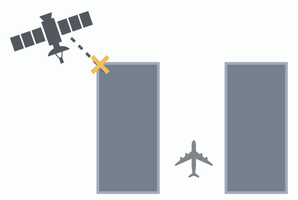
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

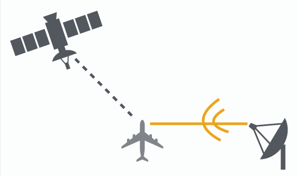




Multipath
Reflections from building faces bias position estimation



Blockage
Urban canyons create gaps and unstable fixes



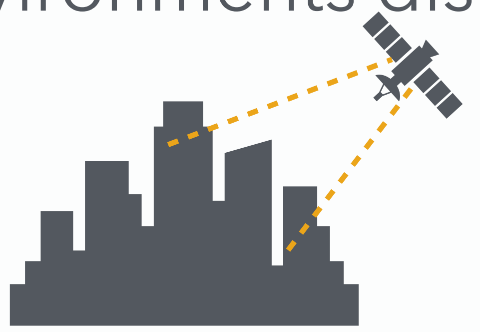
Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

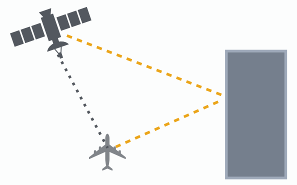
2. CONSEQUENCE

GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

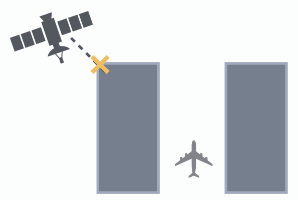
Urban environments disrupt navigation integrity





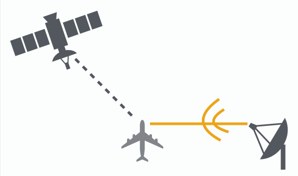
Multipath

Reflections from building faces bias position estimation



Blockage

Urban canyons create gaps and unstable fixes



Spoofing / jamming

Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

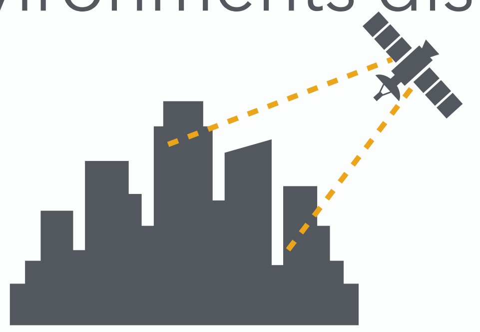
A closing conflict can be reported as clear traffic

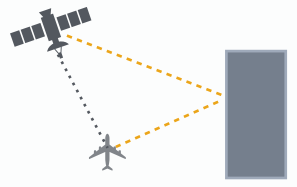
02 THE PROBLEM

GNSS degradation distorts the state the policy relies on

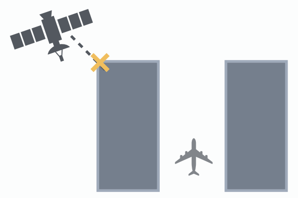
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

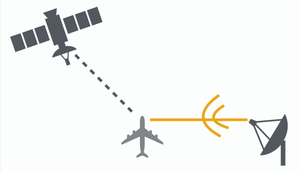




Multipath
Reflections from building faces bias position estimation



Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

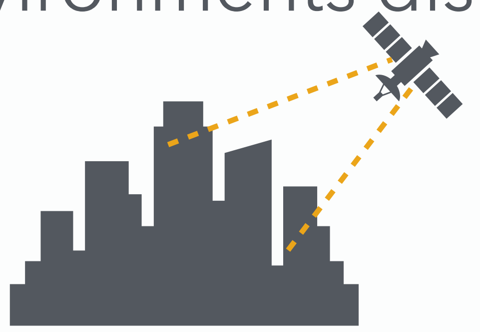
2. CONSEQUENCE

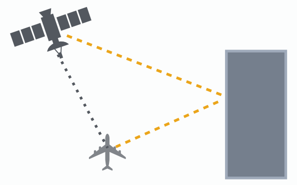
A closing conflict can be reported as clear traffic

GNSS degradation distorts the state the policy relies on

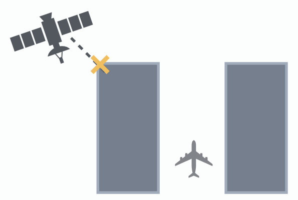
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

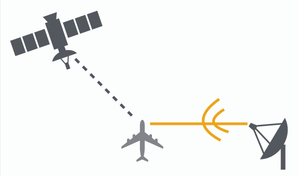




Multipath
Reflections from building faces bias position estimation



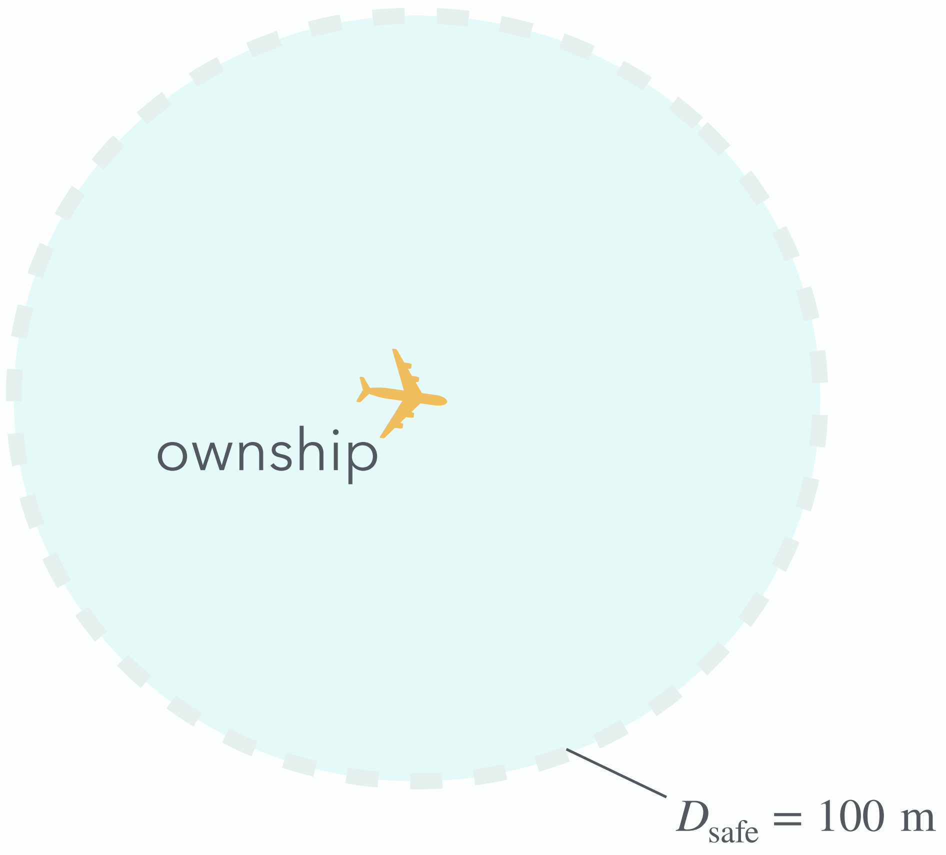
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

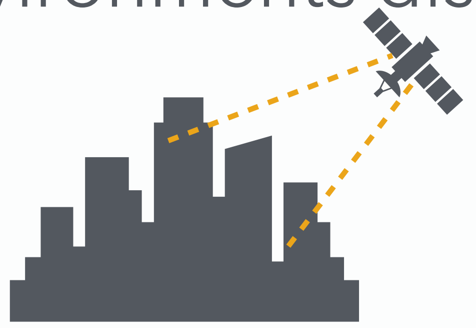
A closing conflict can be reported as clear traffic

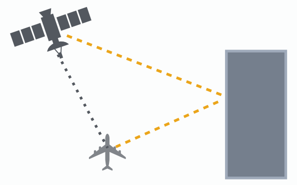


GNSS degradation distorts the state the policy relies on

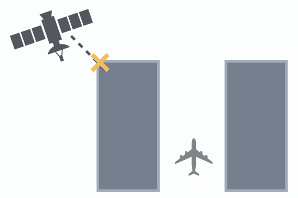
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

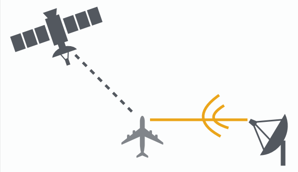




Multipath
Reflections from building faces bias position estimation



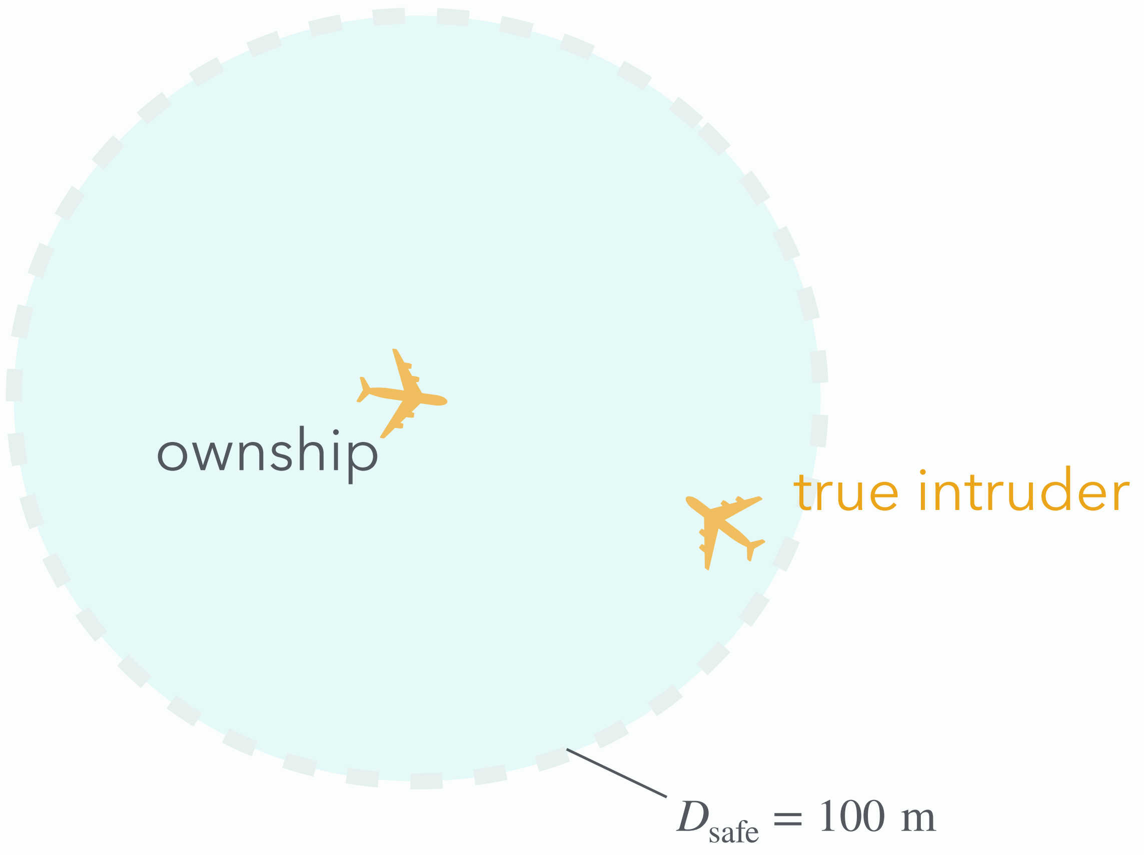
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

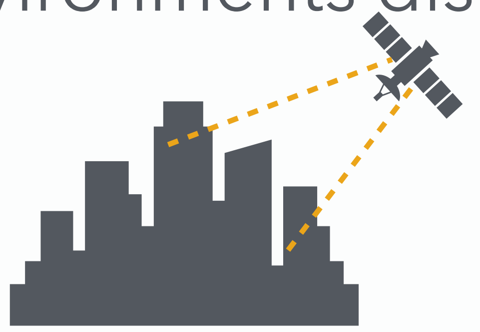
A closing conflict can be reported as clear traffic

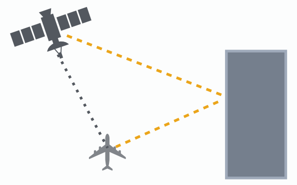


GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

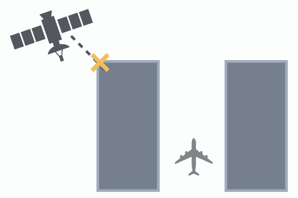
Urban environments disrupt navigation integrity





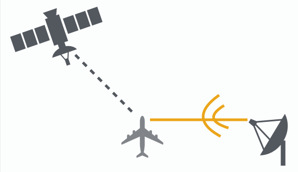
Multipath

Reflections from building faces bias position estimation



Blockage

Urban canyons create gaps and unstable fixes

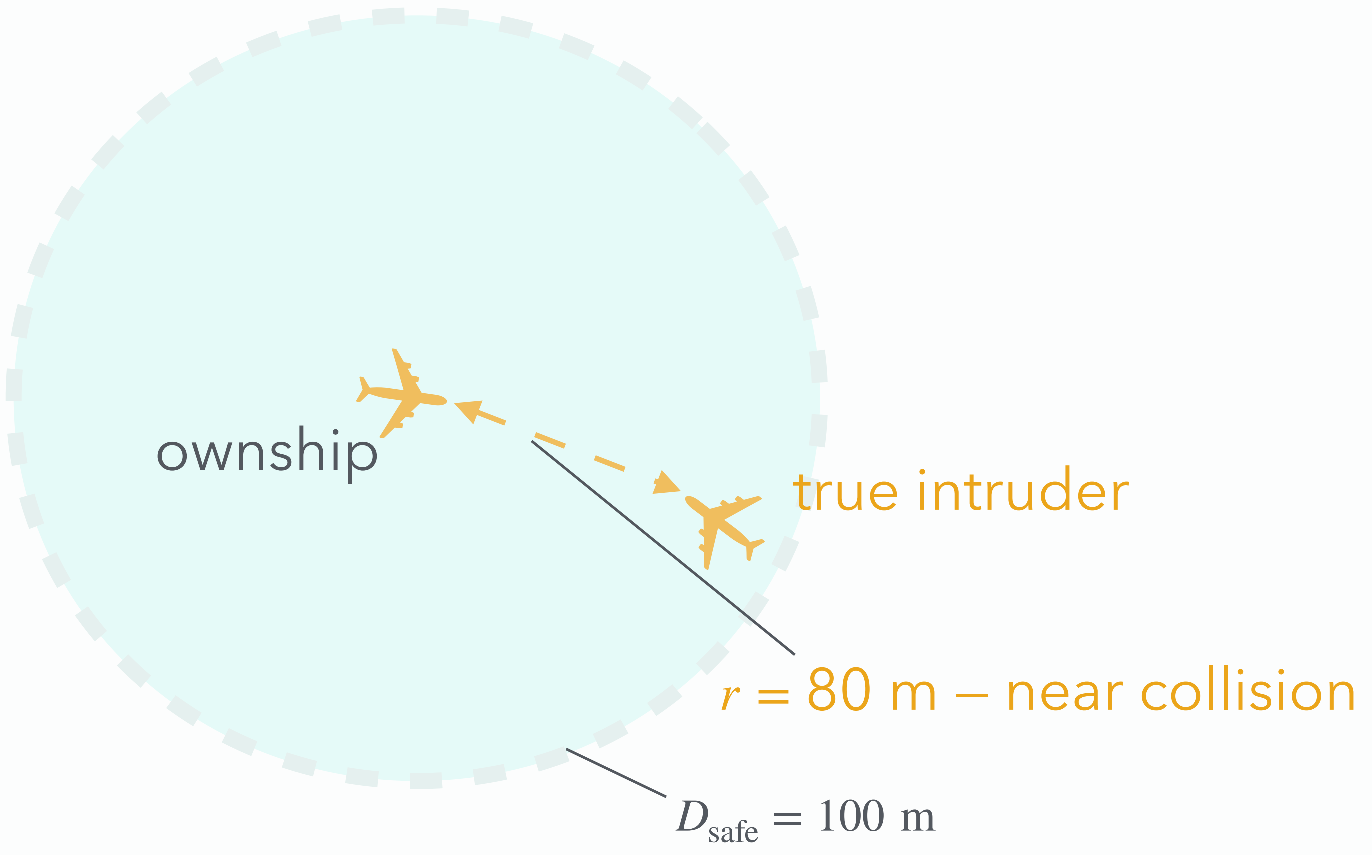


Spoofing / jamming

Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

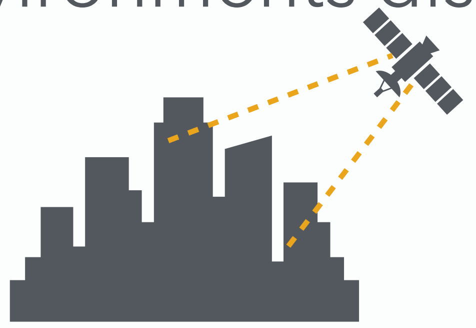
A closing conflict can be reported as clear traffic

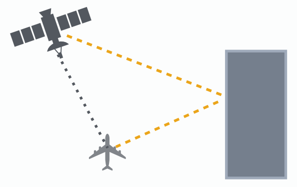


GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

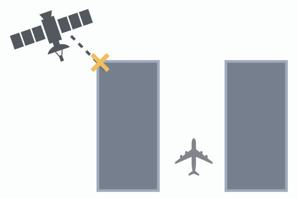
Urban environments disrupt navigation integrity





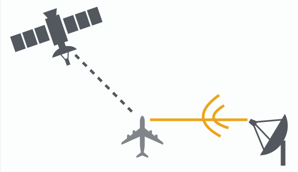
Multipath

Reflections from building faces bias position estimation



Blockage

Urban canyons create gaps and unstable fixes

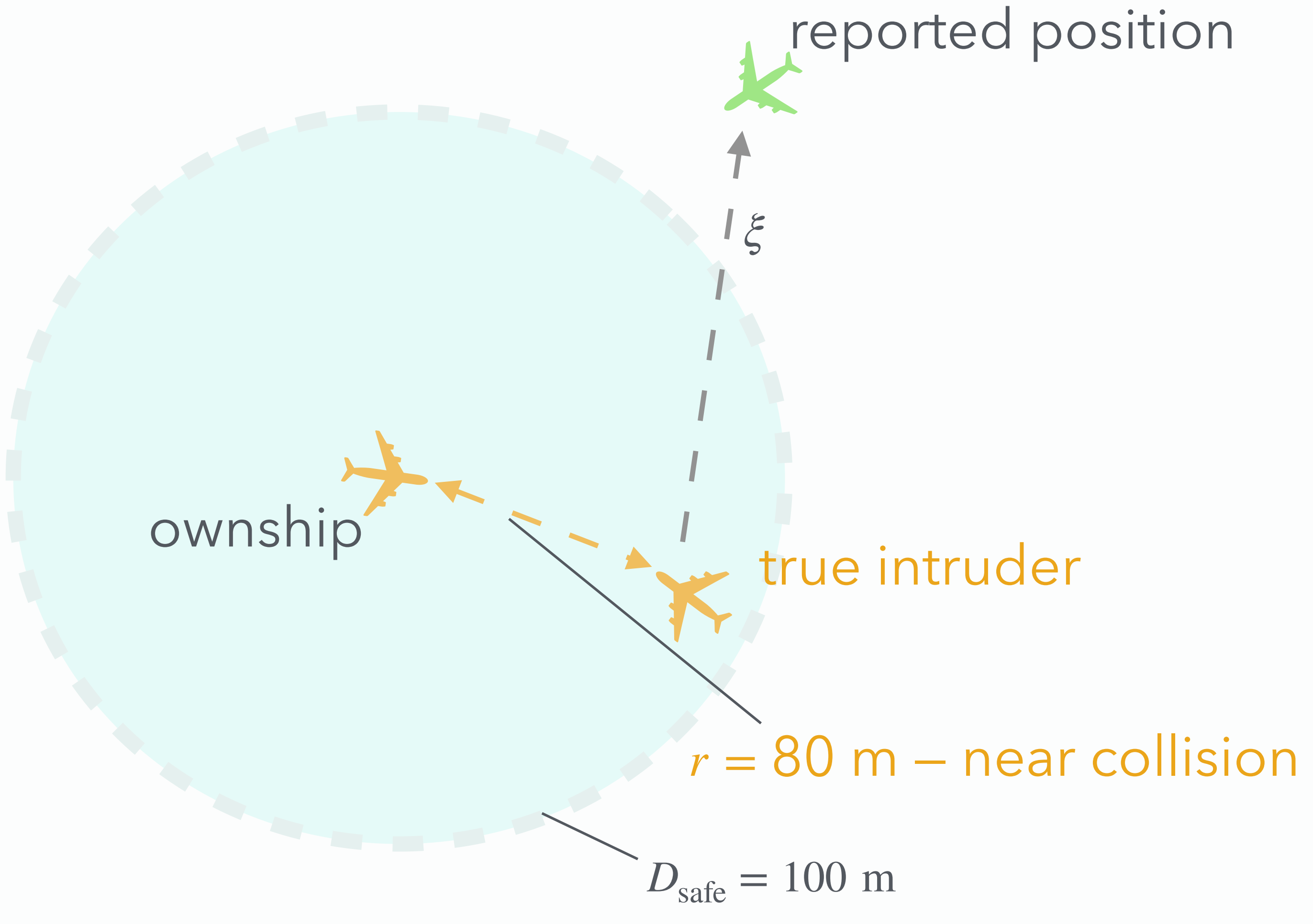


Spoofing / jamming

Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

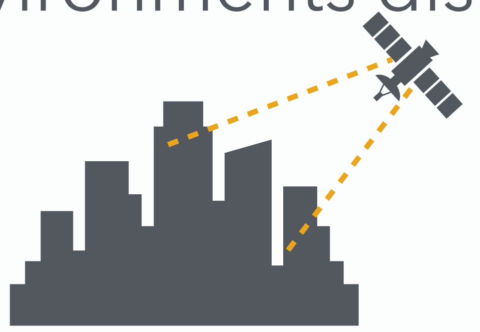
A closing conflict can be reported as clear traffic

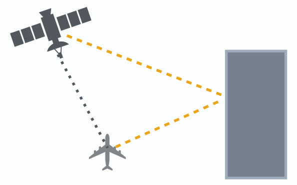


GNSS degradation distorts the state the policy relies on

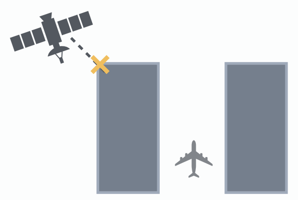
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

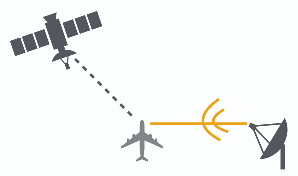




Multipath
Reflections from building faces bias position estimation



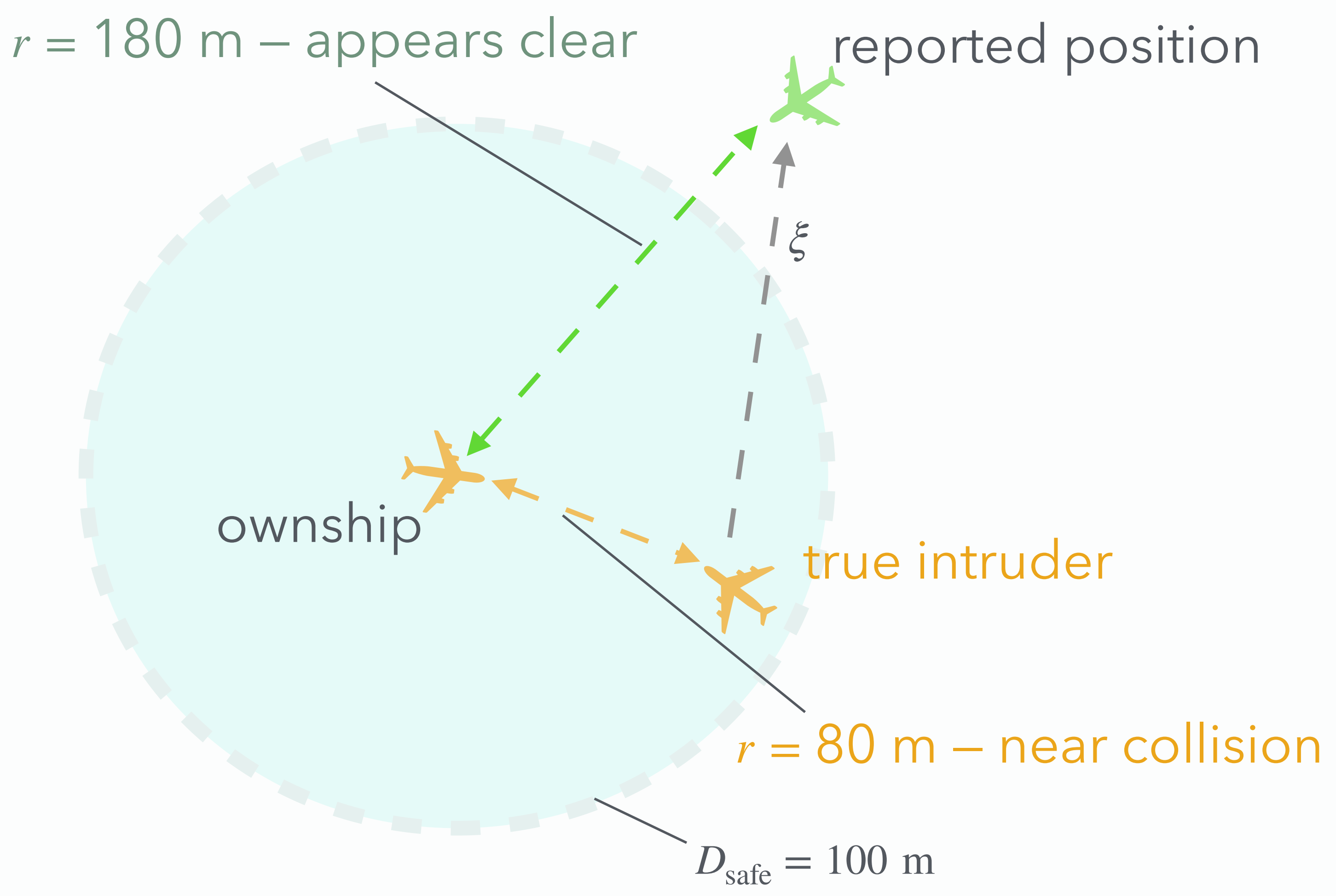
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

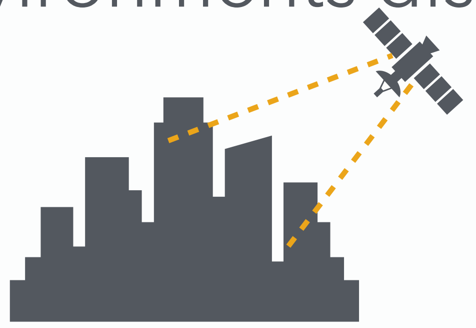
A closing conflict can be reported as clear traffic

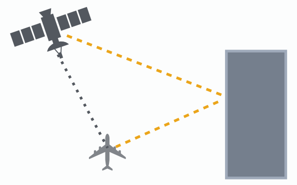


GNSS degradation distorts the state the policy relies on

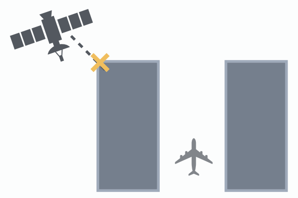
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

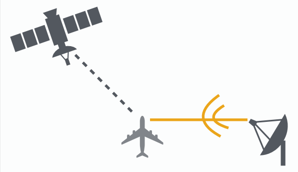




Multipath
Reflections from building faces bias position estimation



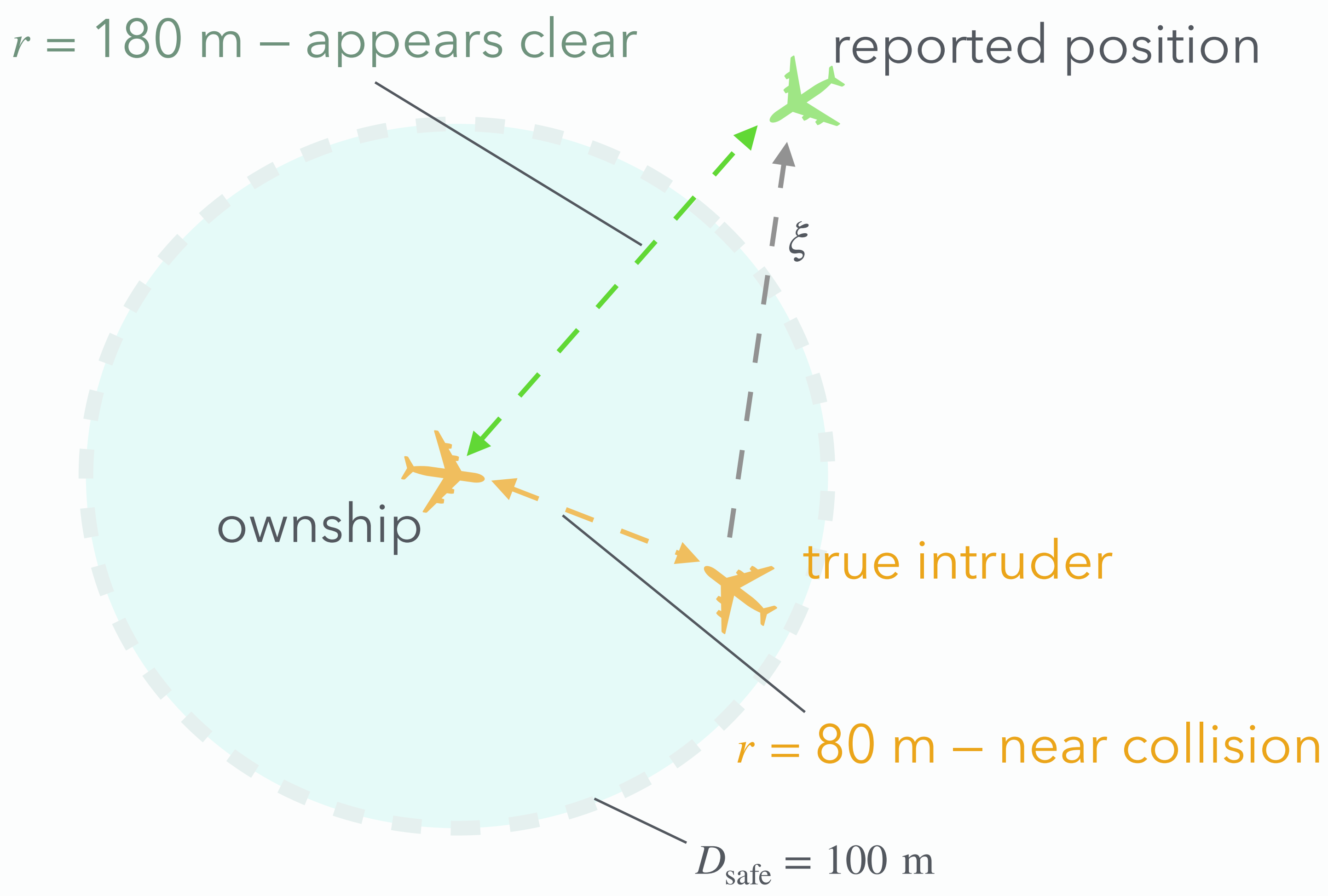
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

A closing conflict can be reported as clear traffic

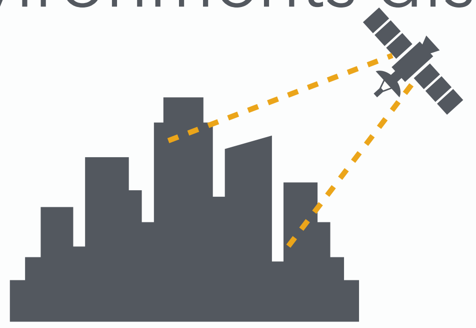


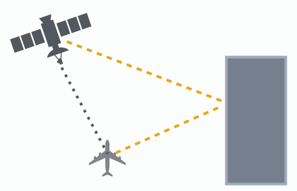
3. DEGRADATION MODEL

GNSS degradation distorts the state the policy relies on

1. WHY URBAN GNSS DEGRADES

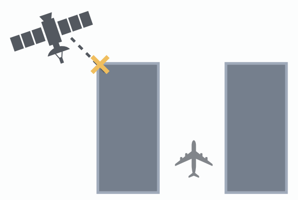
Urban environments disrupt navigation integrity





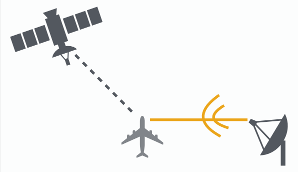
Multipath

Reflections from building faces bias position estimation



Blockage

Urban canyons create gaps and unstable fixes

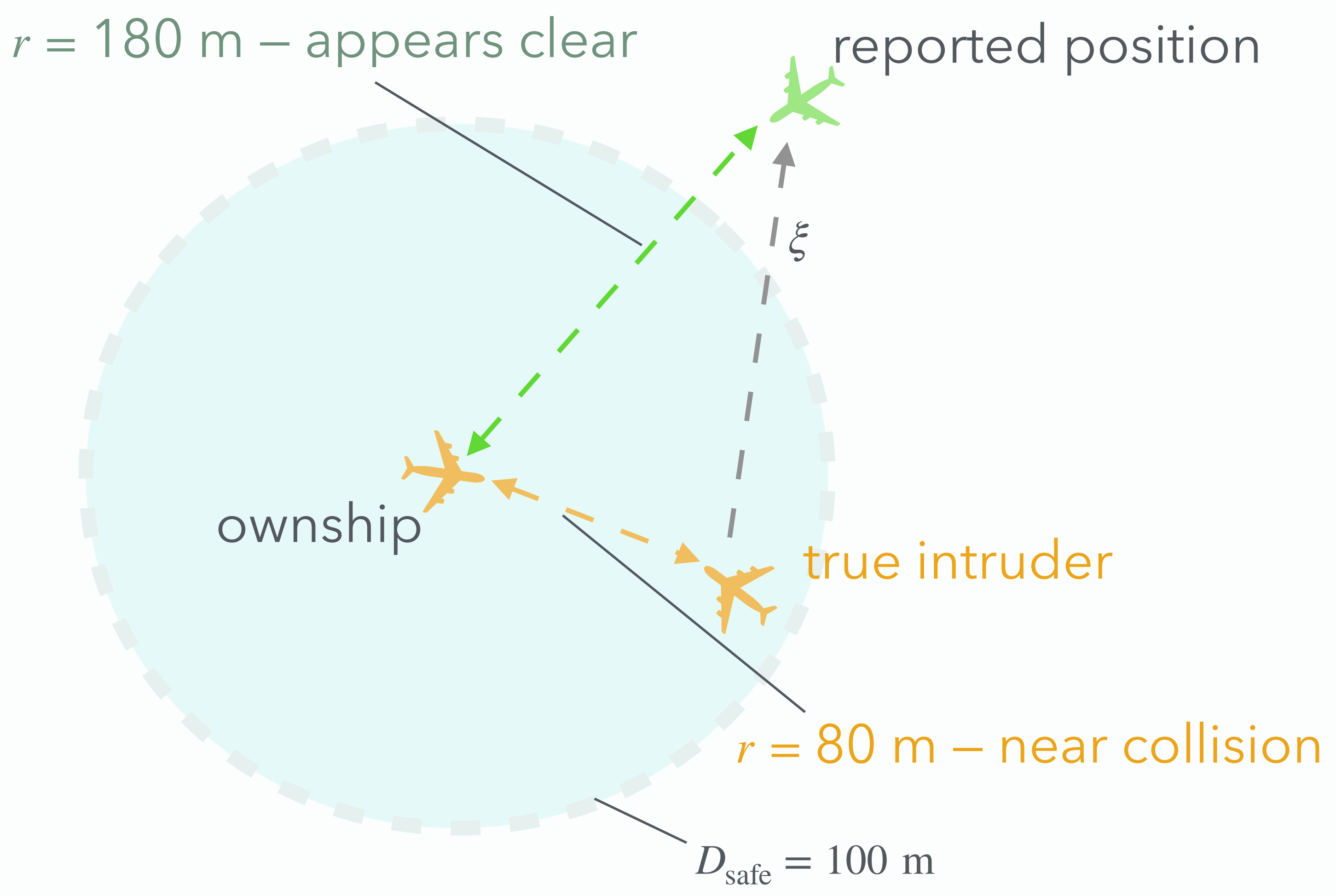


Spoofing / jamming

Delayed signals, false or replayed signals, indistinguishable from the truth

2. CONSEQUENCE

A closing conflict can be reported as clear traffic



3. DEGRADATION MODEL

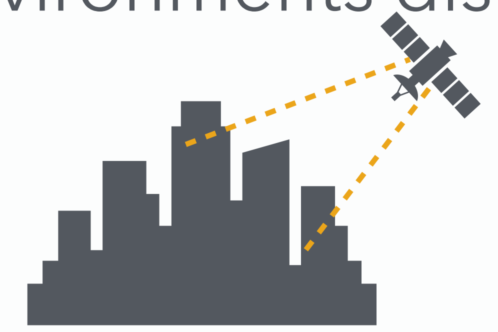
A bounded state degradation model

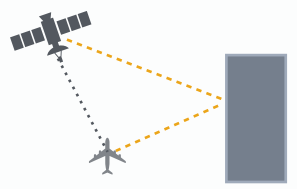
02 THE PROBLEM

GNSS degradation distorts the state the policy relies on

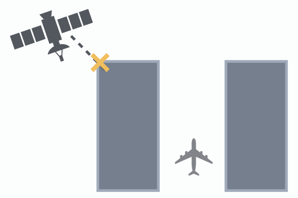
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

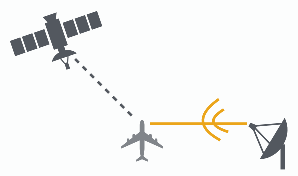




Multipath
Reflections from building faces bias position estimation



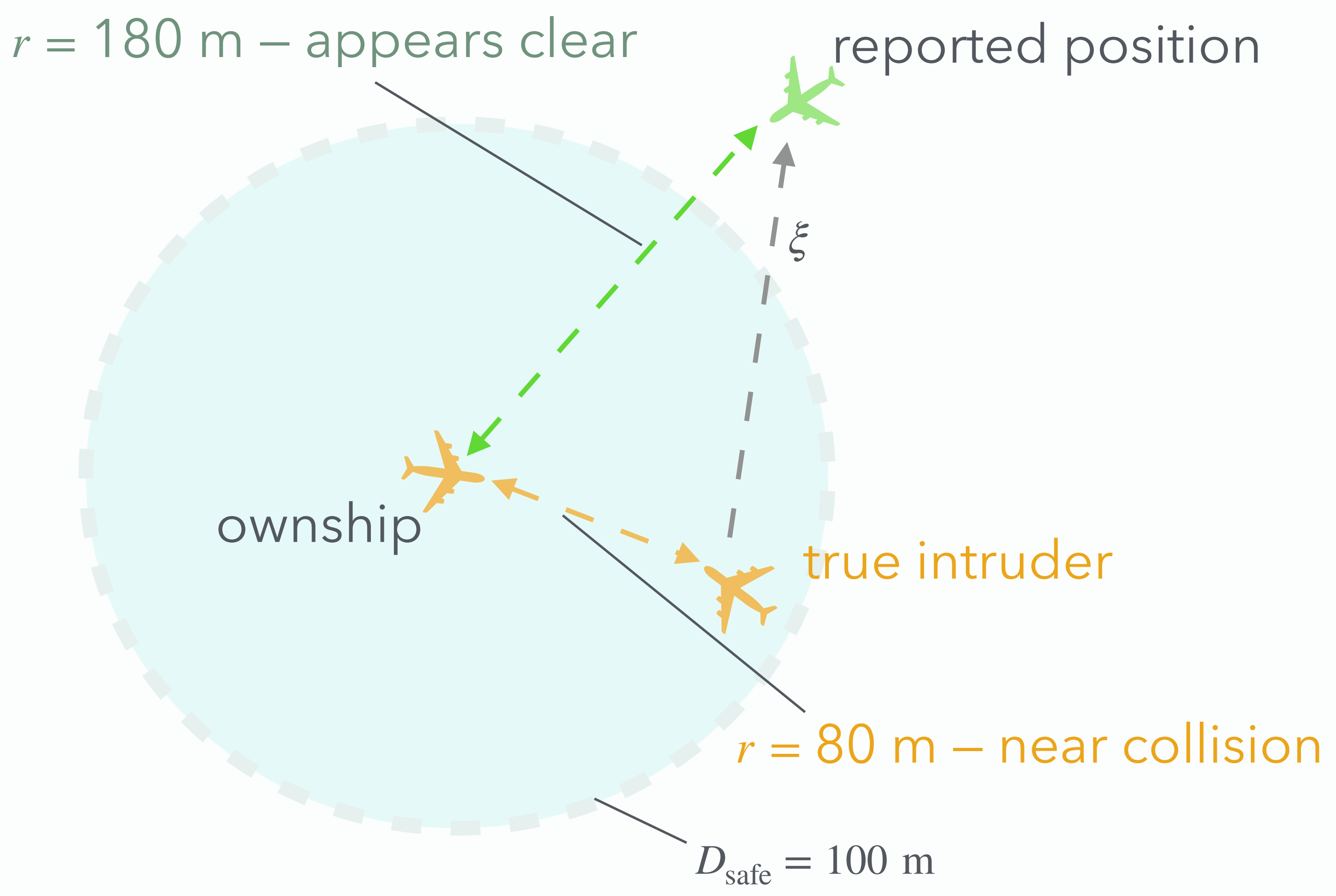
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

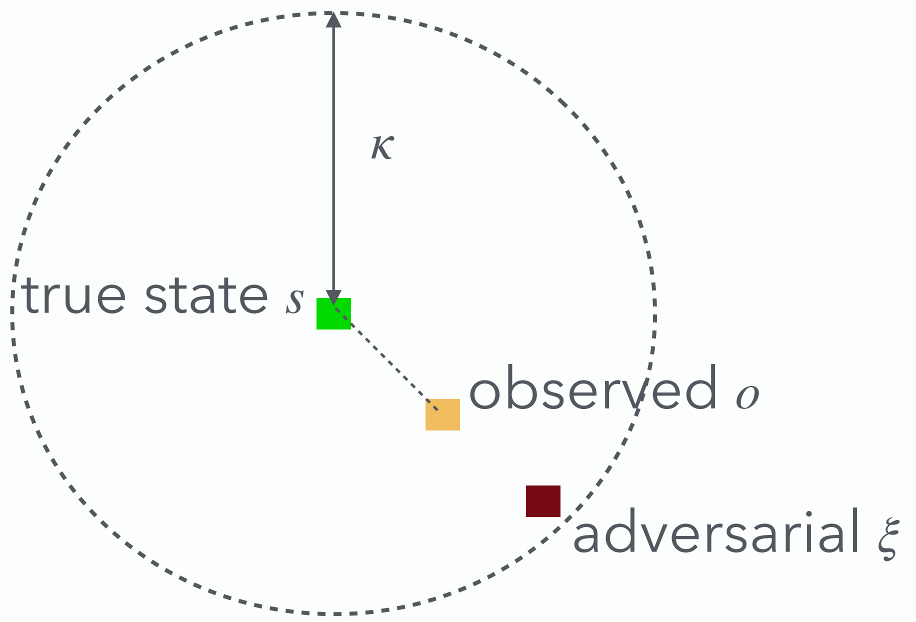
2. CONSEQUENCE

A closing conflict can be reported as clear traffic



3. DEGRADATION MODEL

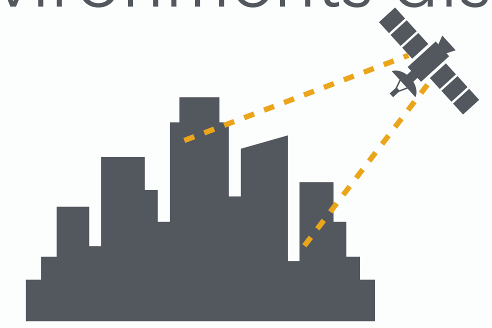
A bounded state degradation model

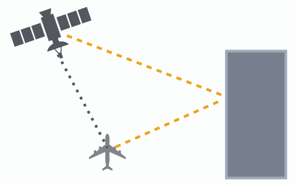


GNSS degradation distorts the state the policy relies on

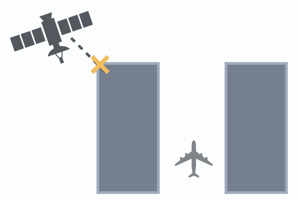
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

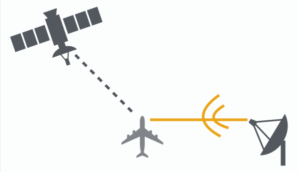




Multipath
Reflections from building faces bias position estimation



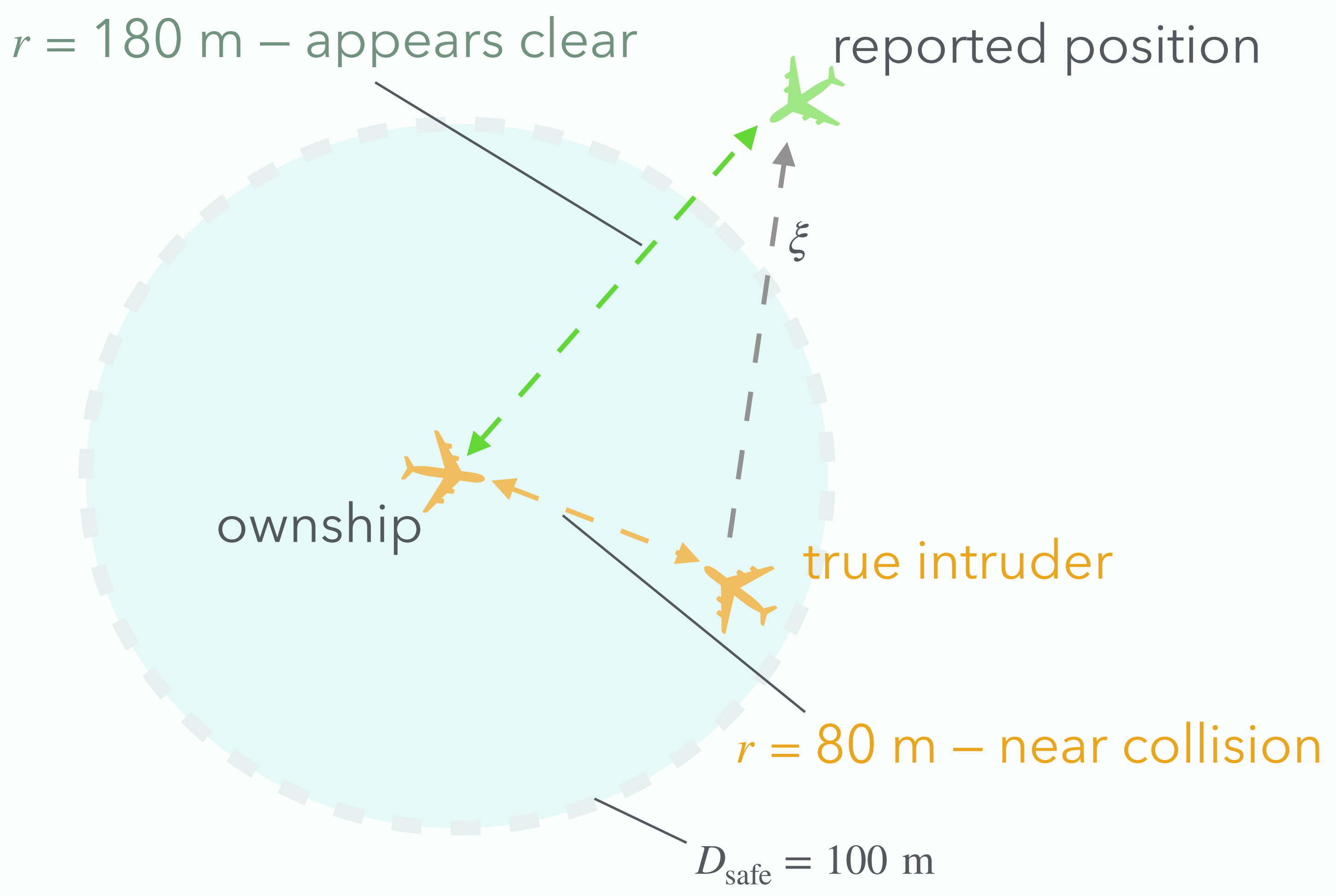
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

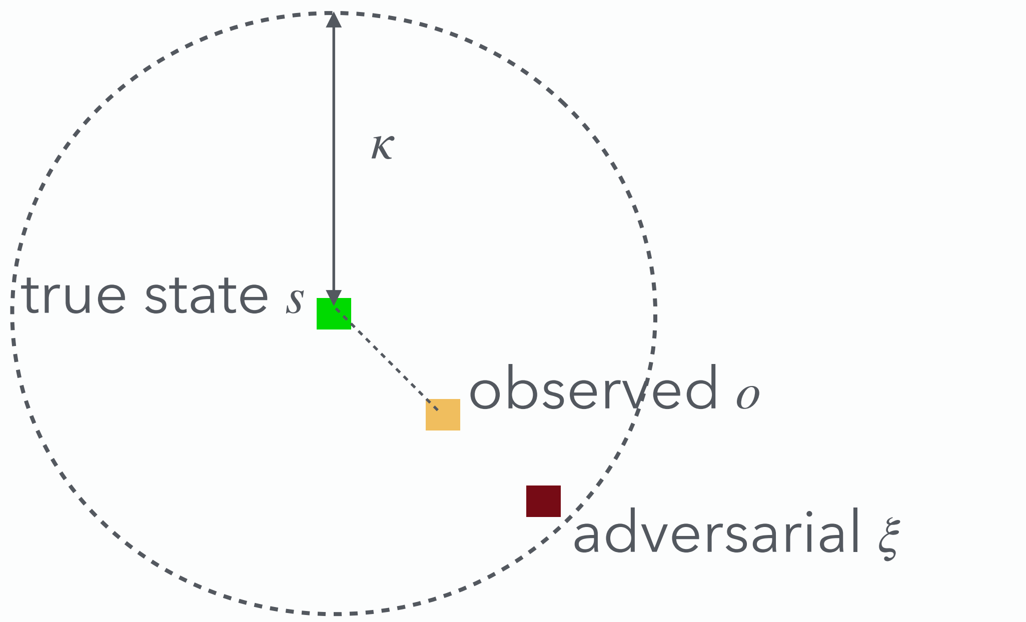
2. CONSEQUENCE

A closing conflict can be reported as clear traffic



3. DEGRADATION MODEL

A bounded state degradation model



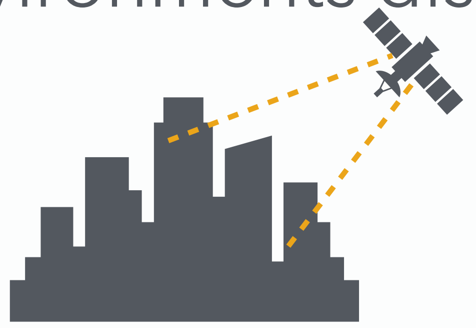
$o = (1 - \mathrm{R})s + \mathrm{R}\xi$, where $\|\xi - s\|_\infty \leqslant \kappa$

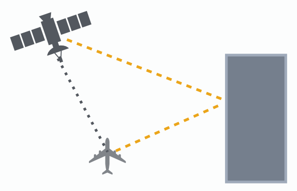
Perturbation is bounded componentwise

GNSS degradation distorts the state the policy relies on

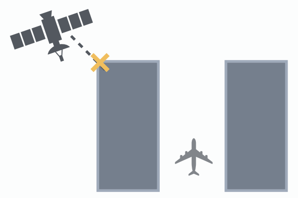
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

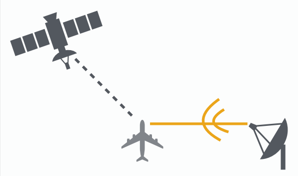




Multipath
Reflections from building faces bias position estimation



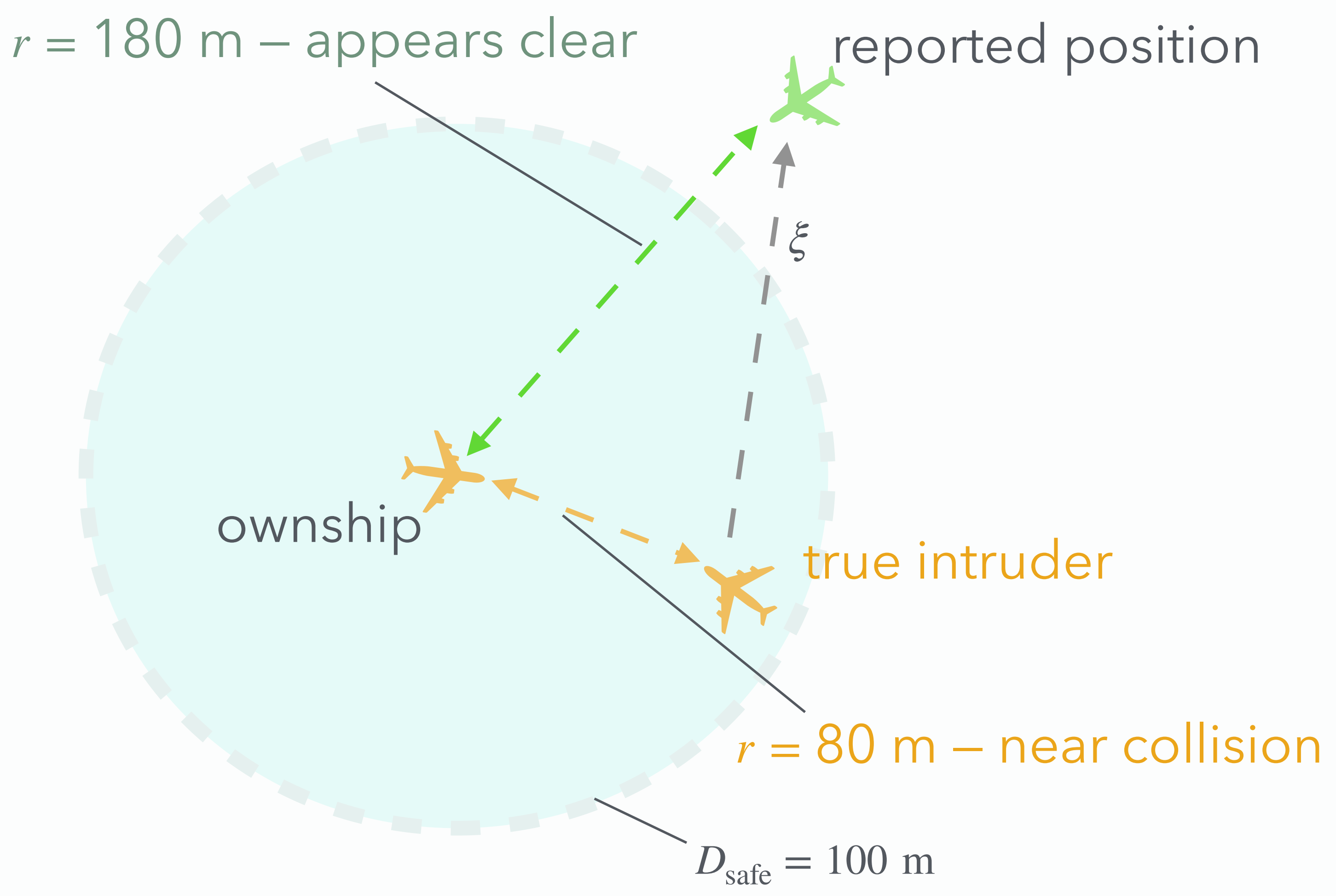
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

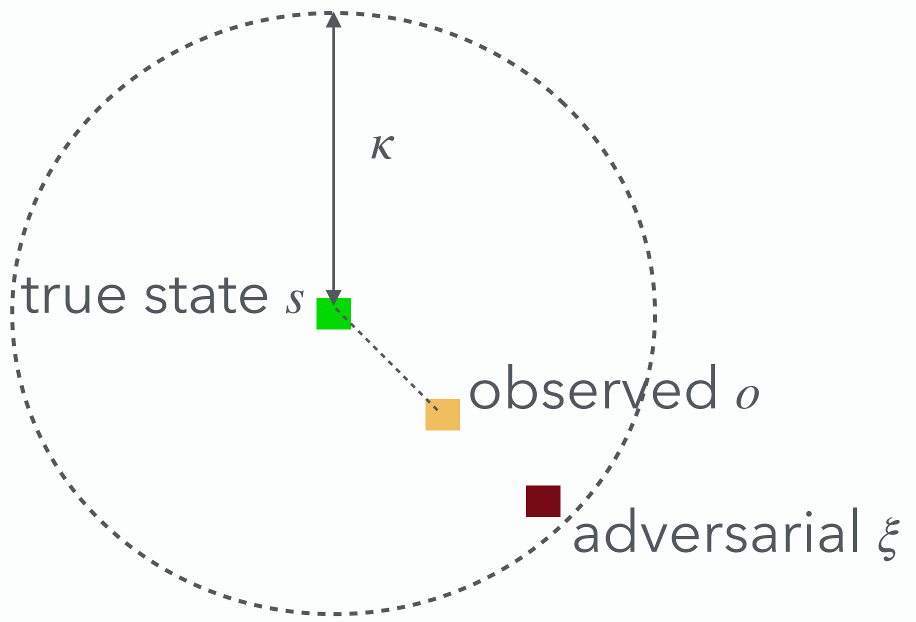
2. CONSEQUENCE

A closing conflict can be reported as clear traffic



3. DEGRADATION MODEL

A bounded state degradation model



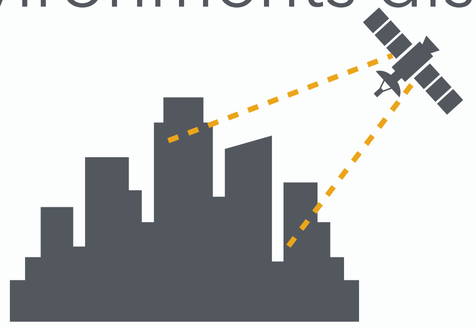
$o = (1 - \mathrm{R})s + \mathrm{R}\xi$, where $\|\xi - s\|_\infty \leqslant \kappa$
Perturbation is bounded componentwise

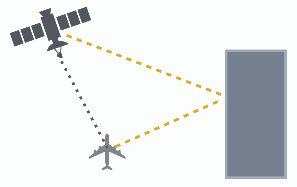
$\mathrm{R} = 0$ · nominal $\mathrm{R} \uparrow$ · degraded

GNSS degradation distorts the state the policy relies on

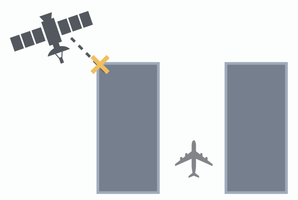
1. WHY URBAN GNSS DEGRADES

Urban environments disrupt navigation integrity

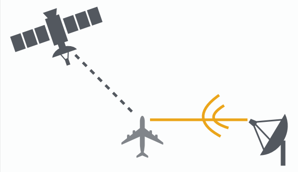




Multipath
Reflections from building faces bias position estimation



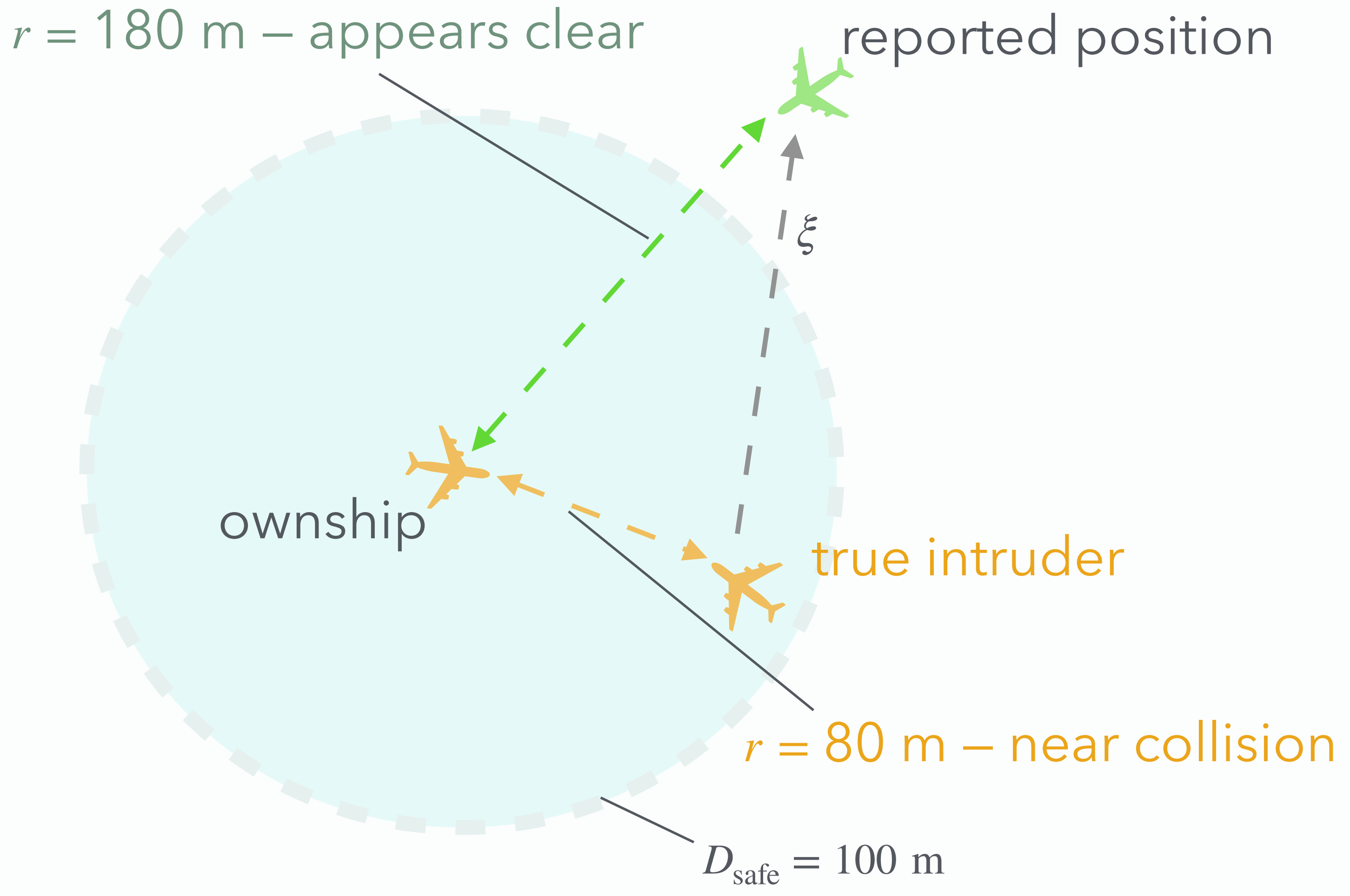
Blockage
Urban canyons create gaps and unstable fixes



Spoofing / jamming
Delayed signals, false or replayed signals, indistinguishable from the truth

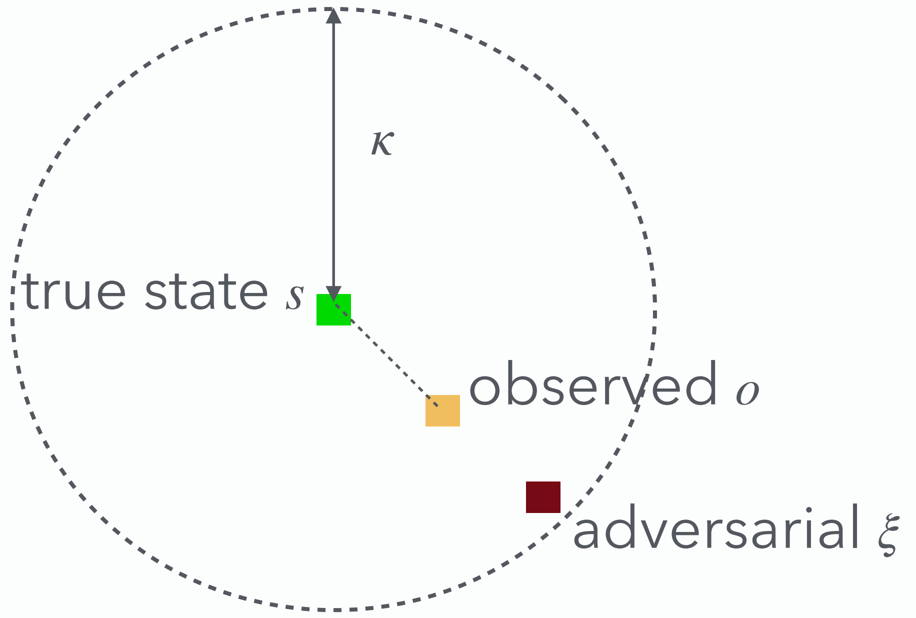
2. CONSEQUENCE

A closing conflict can be reported as clear traffic



3. DEGRADATION MODEL

A bounded state degradation model



$o = (1 - \mathrm{R})s + \mathrm{R}\xi$, where $\|\xi - s\|_\infty \leqslant \kappa$

Perturbation is bounded componentwise

$\mathrm{R} = 0$ · nominal — $\mathrm{R}\uparrow$ · degraded

The separation policy then acts on observation o, while safety is measured on true state s.

Robustness can be built in – or handled at runtime

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained
- Requires no retraining of the deployed policy

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained
- Requires no retraining of the deployed policy
- Uses the current degradation bound at each decision step

02 THE PROBLEM

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained
- Requires no retraining of the deployed policy
- Uses the current degradation bound at each decision step
- Has no training-time knowledge and inherits whatever the policy learned

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained
- Requires no retraining of the deployed policy
- Uses the current degradation bound at each decision step
- Has no training-time knowledge and inherits whatever the policy learned

How should a runtime filter attach to a learned policy?

Robustness can be built in – or handled at runtime

ADVERSARIAL / ROBUST TRAINING

- Shapes how the policy responds to corrupted or threatening observations
- Robustness depends on the assumed disturbances and training distribution
- A train-deployment gap can remain when real degradation exceeds those assumptions

RUNTIME FILTERING

- Acts during execution, independent of how the policy was trained
- Requires no retraining of the deployed policy
- Uses the current degradation bound at each decision step
- Has no training-time knowledge and inherits whatever the policy learned

How should a runtime filter attach to a learned policy?

Before the policy sees the state – or after it proposes an action?

Two ways to add a runtime safety filter

Two ways to add a runtime safety filter

Degraded observation o

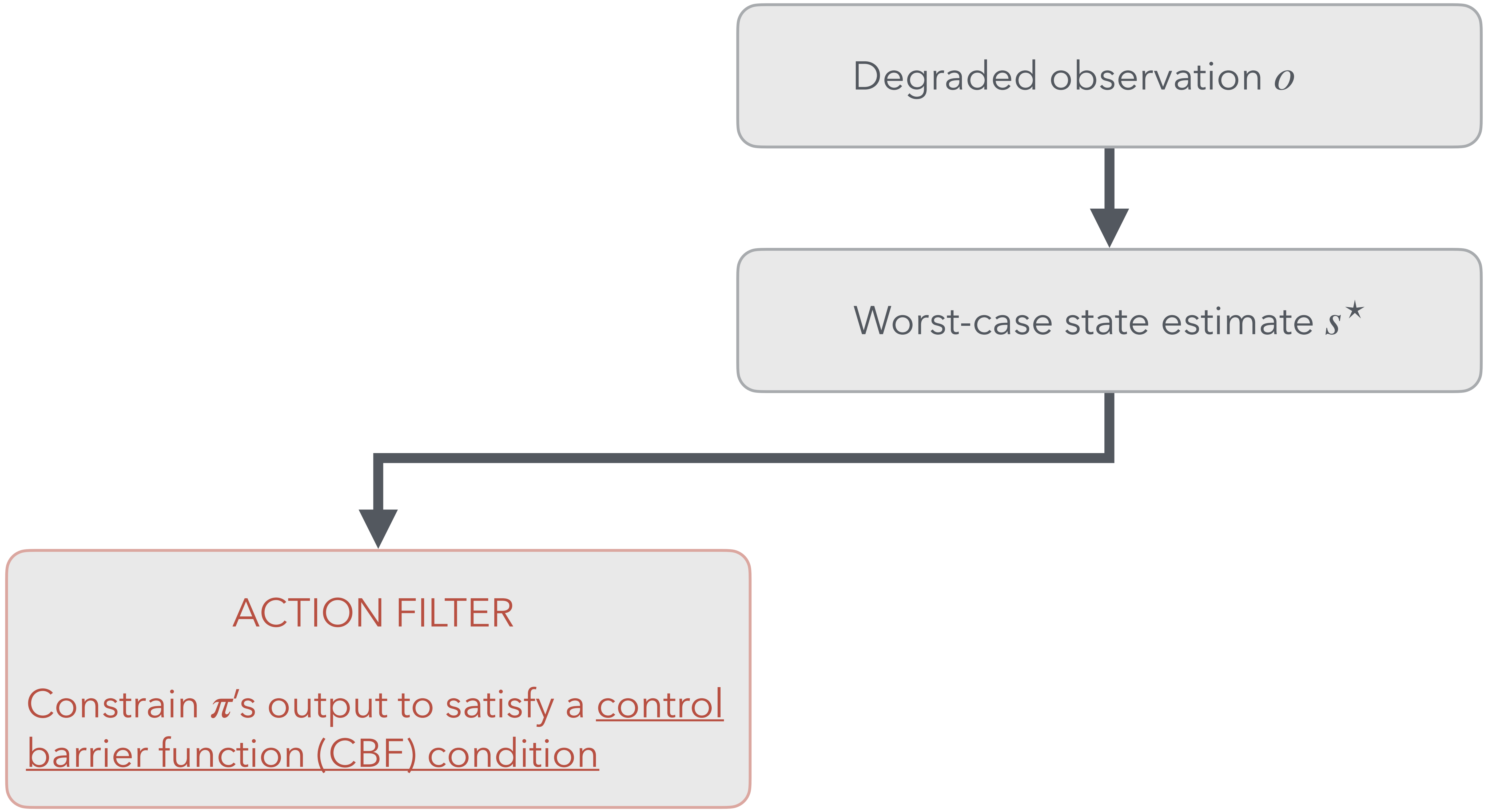
Two ways to add a runtime safety filter

Degraded observation o

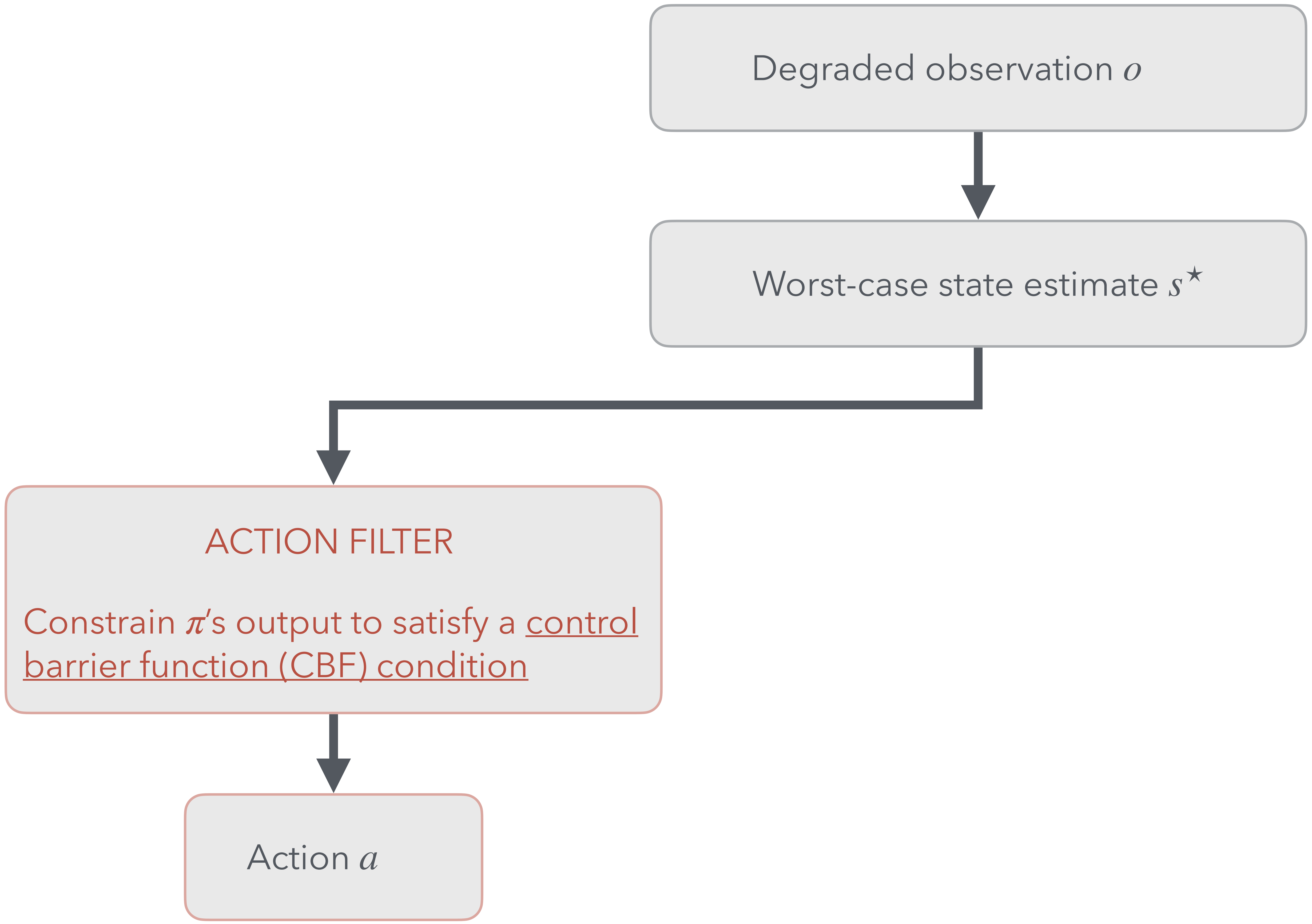
↓

Worst-case state estimate $s^\star$

Two ways to add a runtime safety filter

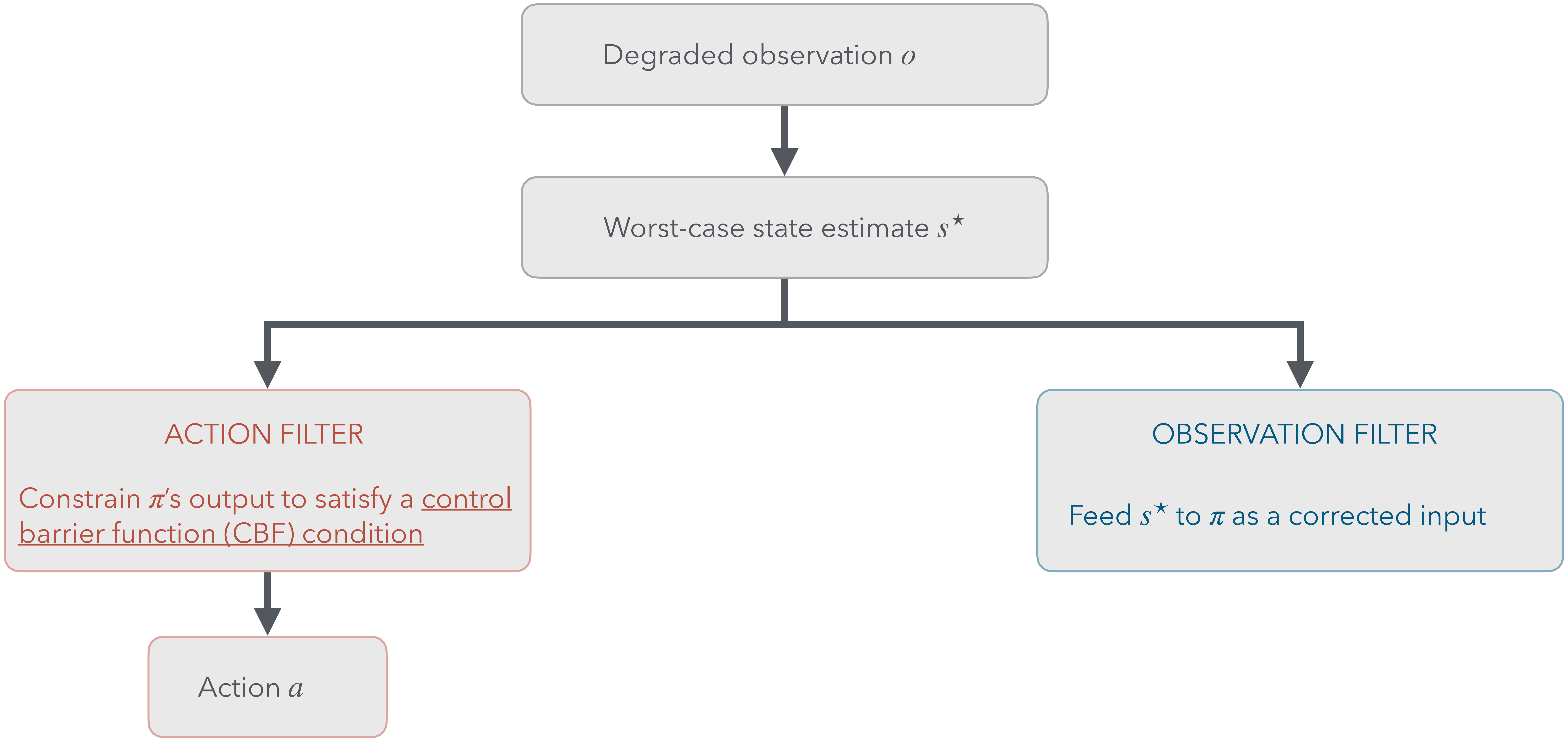


Two ways to add a runtime safety filter

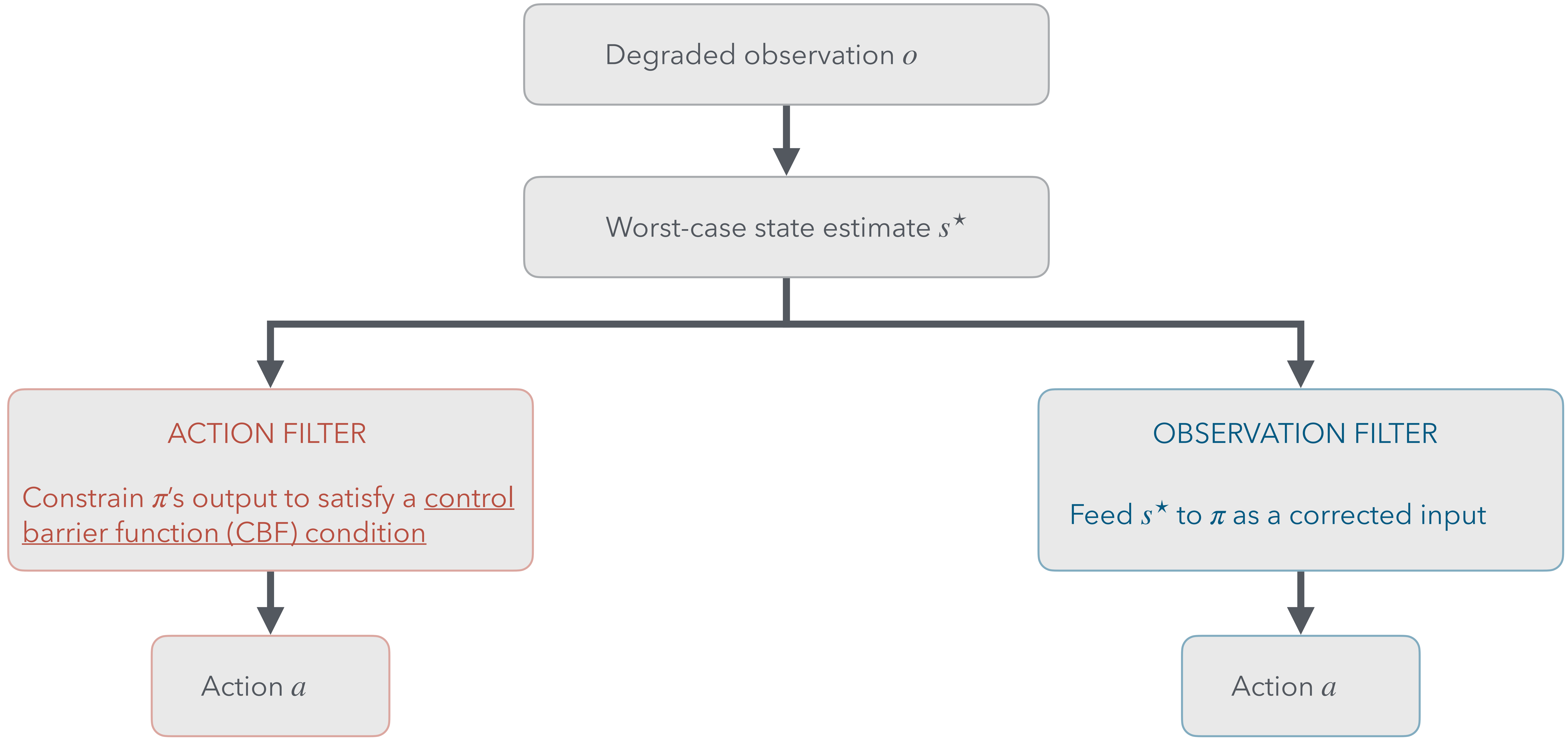


03 APPROACH

Two ways to add a runtime safety filter



Two ways to add a runtime safety filter



Both filters start from the same worst-case state estimation

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Both filters start from the same worst-case state estimation

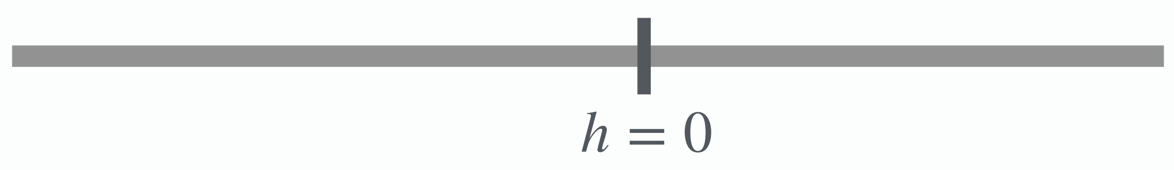
1. SAFETY MARGIN

Barrier function as safety margin

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

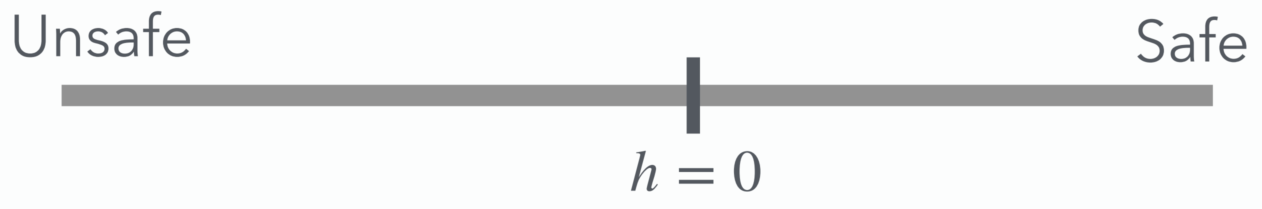
Barrier function as safety margin



Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

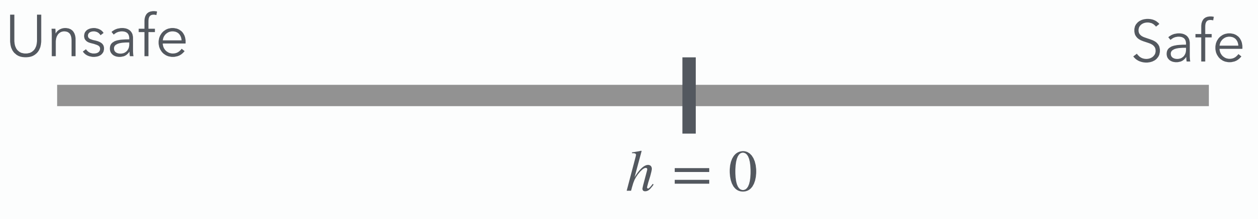
Barrier function as safety margin



Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



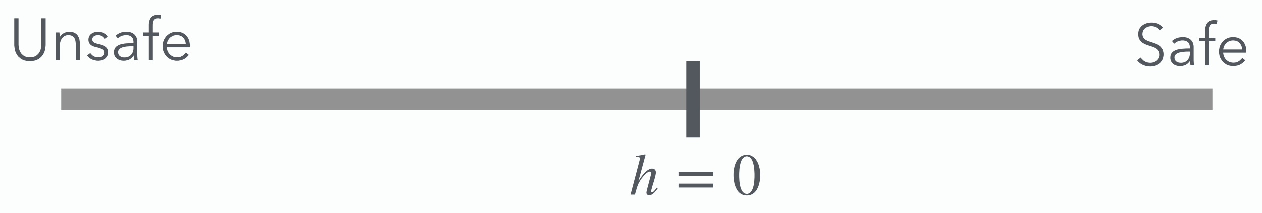
$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

03 APPROACH

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

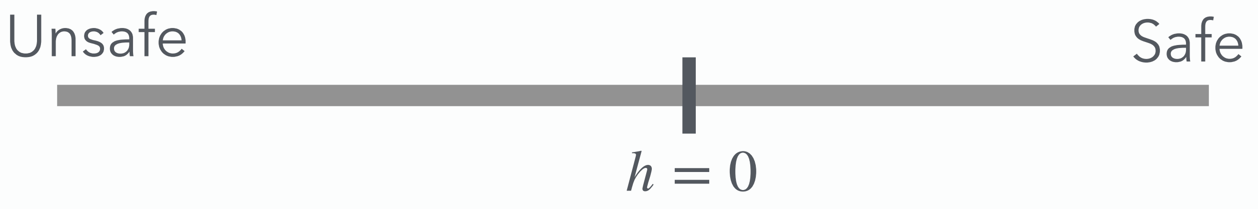
$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

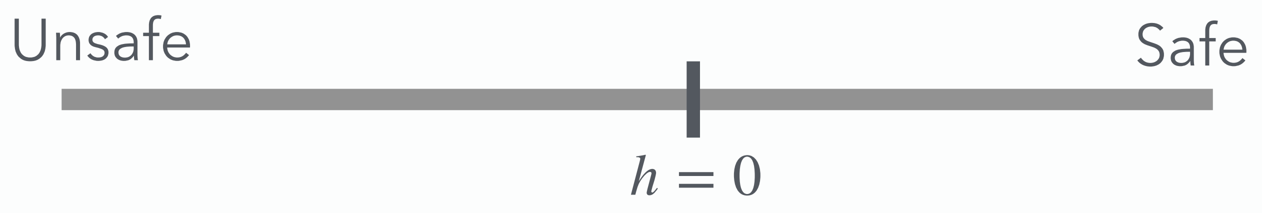
Whether two UASs are closing in on each other
α sets how far ahead the margin looks

03 APPROACH

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

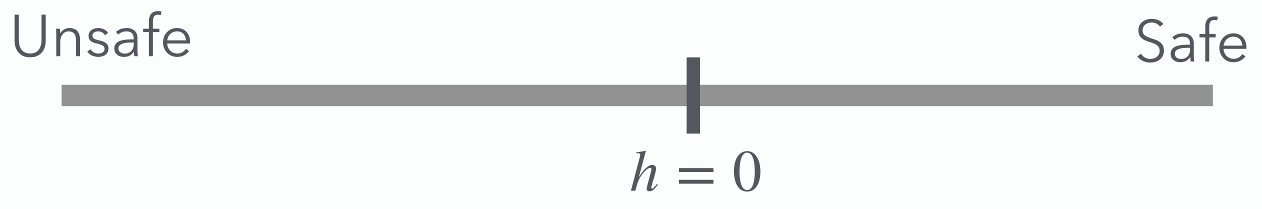
Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

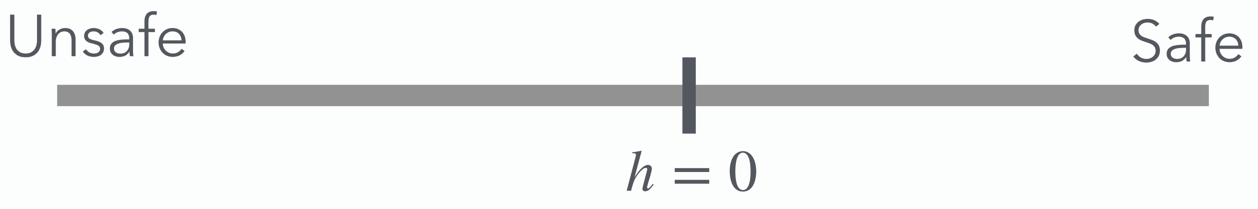
2. WORST CASE

What looked clear now reads as a conflict

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

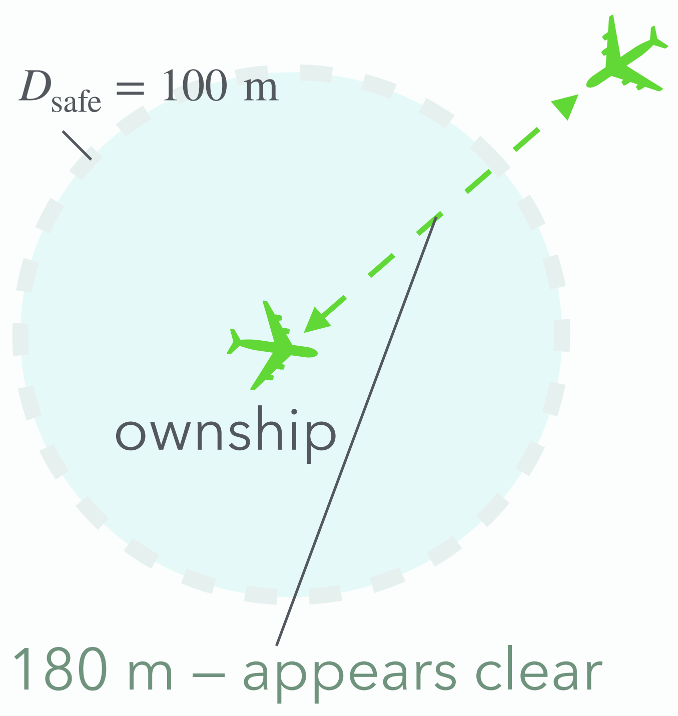
$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict

Current observation



Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin

Unsafe — Safe

$h = 0$

$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

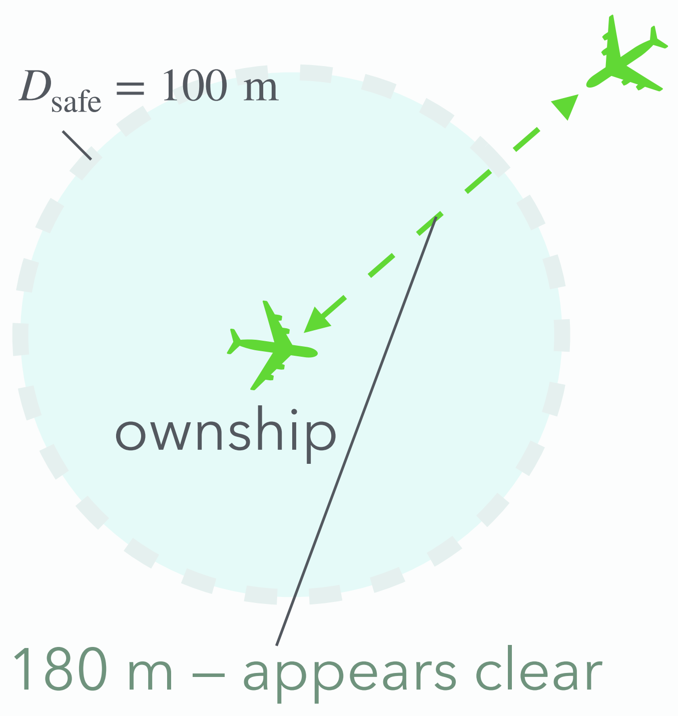
$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict

Current observation

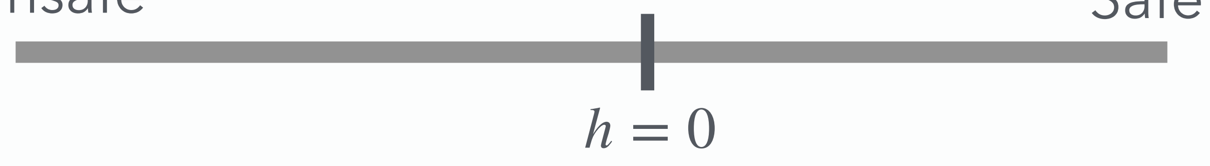


$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, R_{\max})} h(s)$$

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

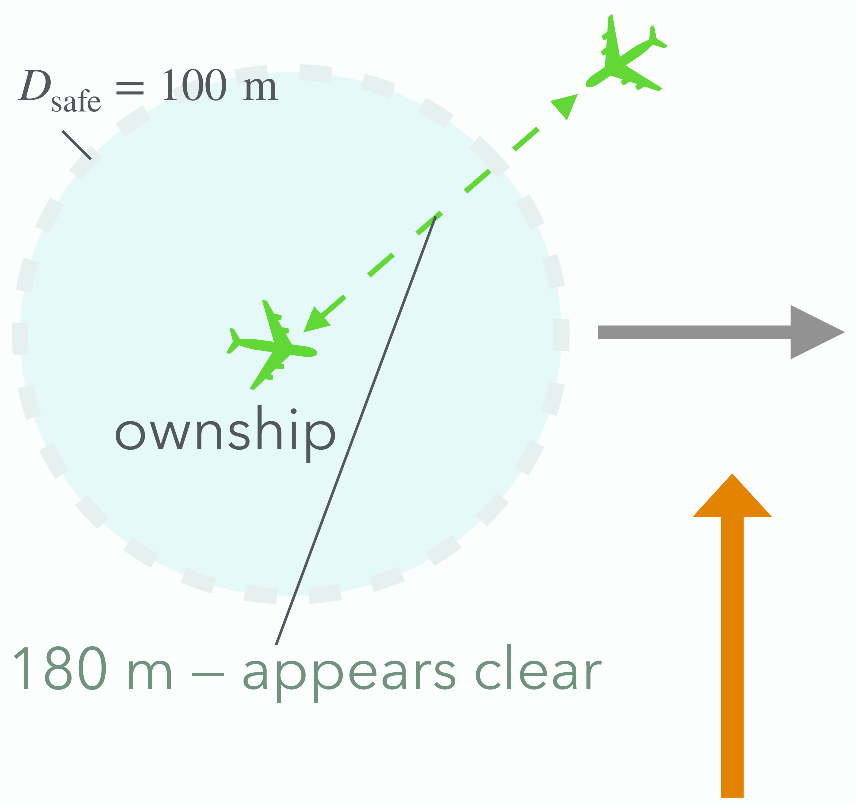
$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict

Current observation

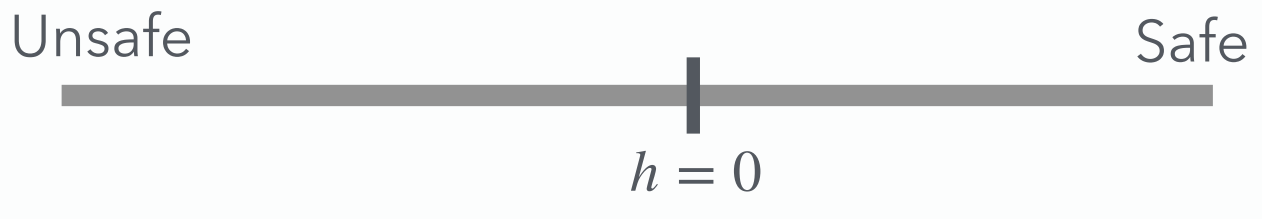


$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

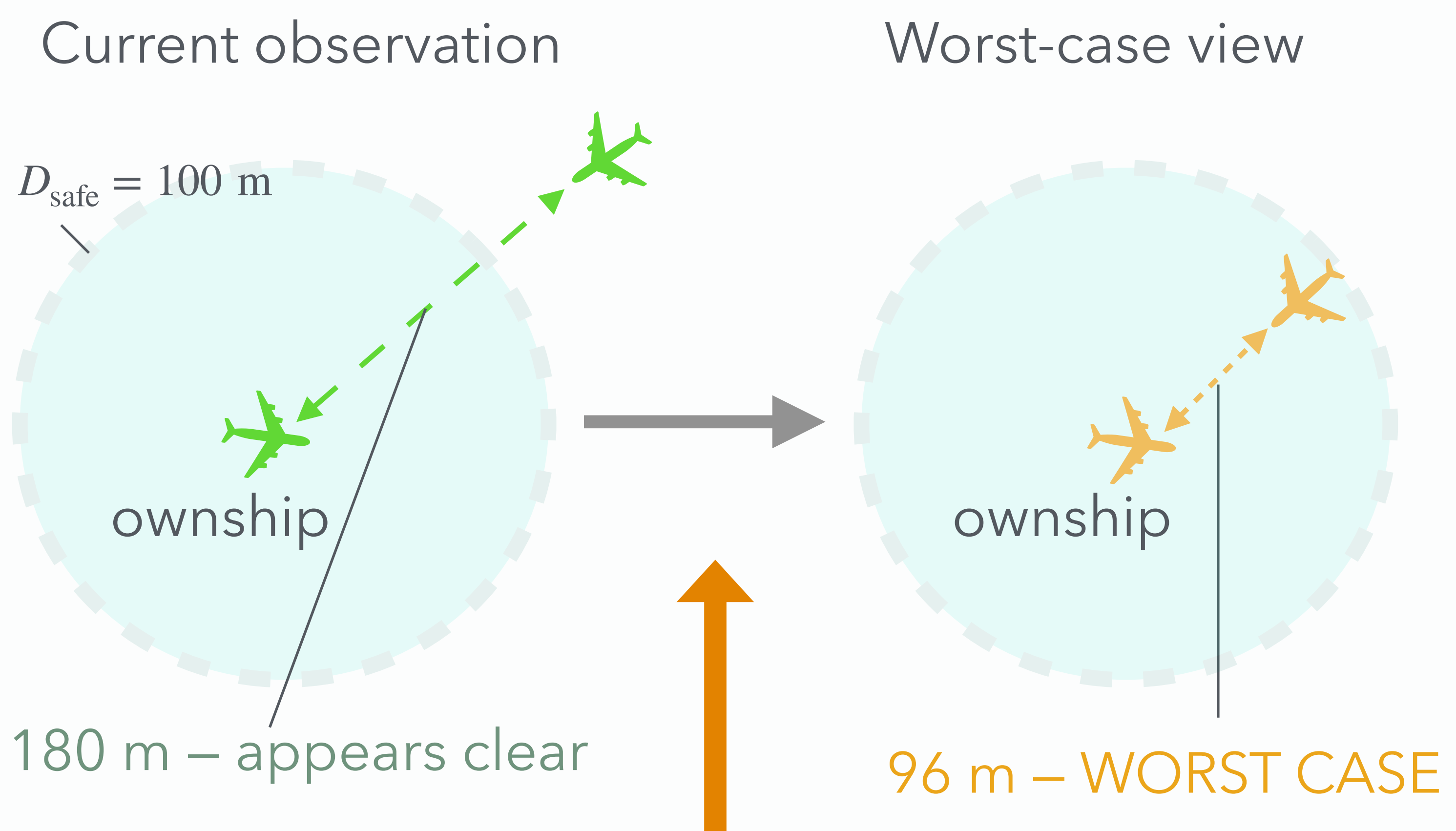
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict



$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin

Unsafe — Safe

$h = 0$

$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

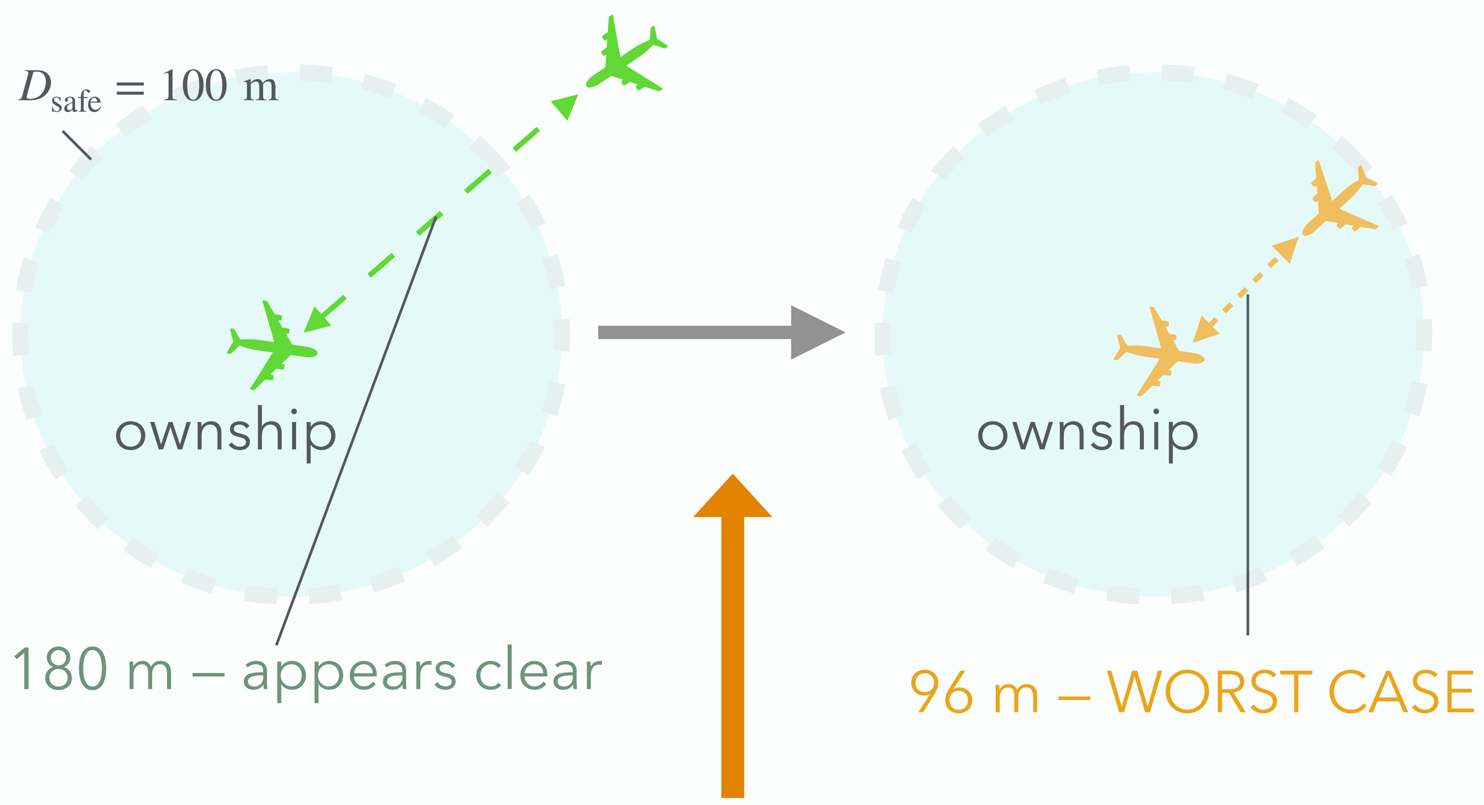
$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict

Current observation — Worst-case view



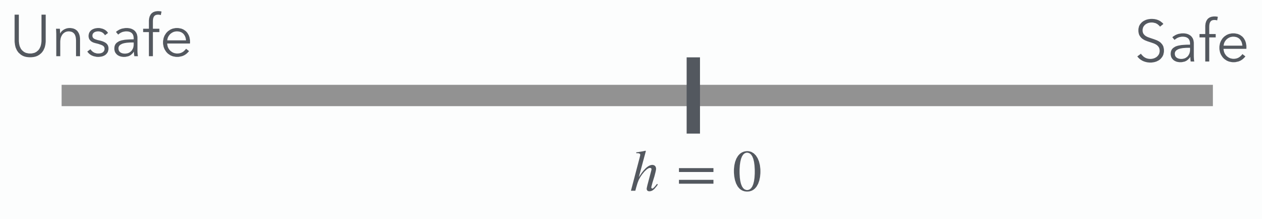
$$s^\star = \arg\min_{s \in \mathcal{U}(o,\, R_{\max})} h(s)$$

3. IN CLOSED FORM

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

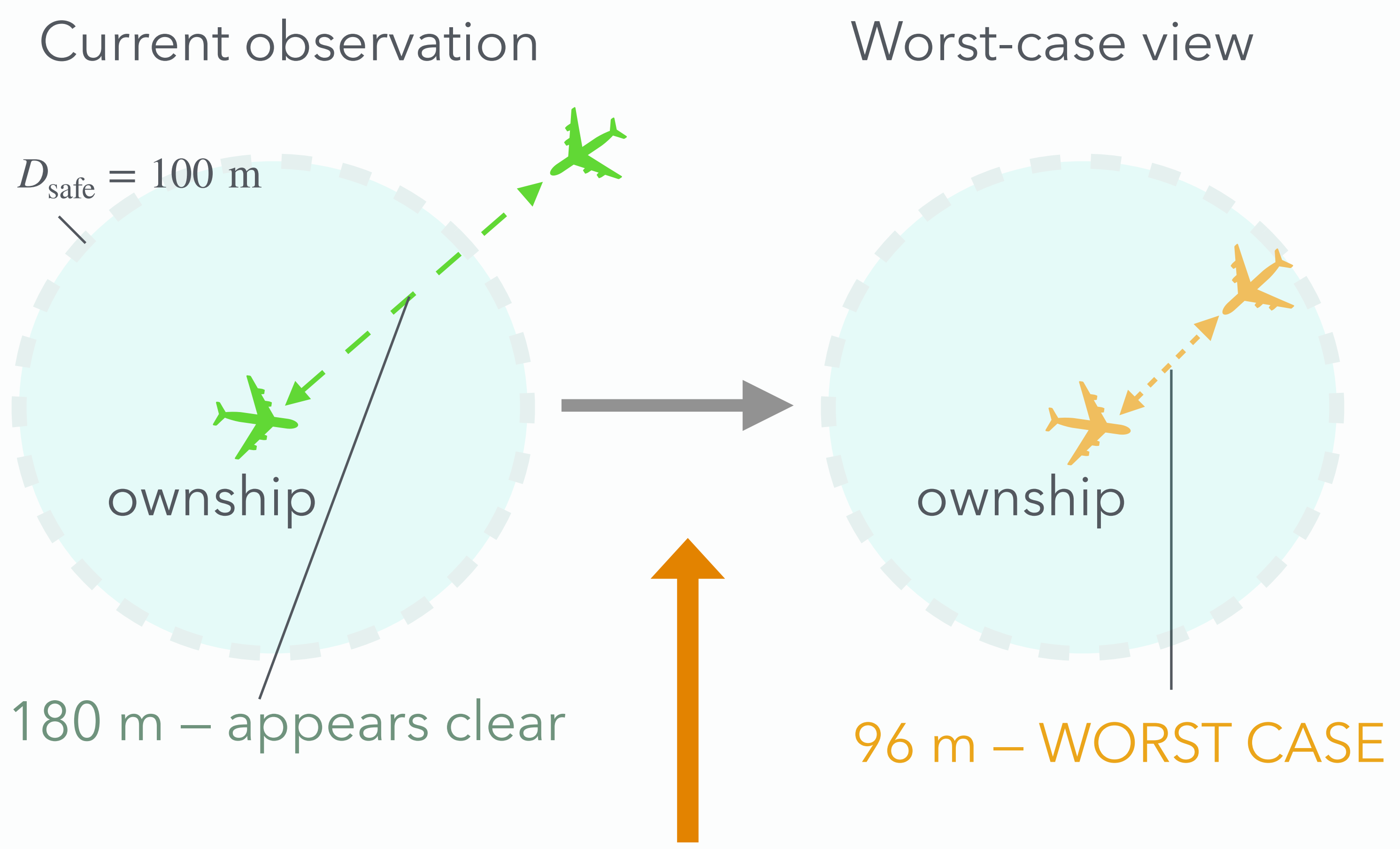
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict



$$s^\star = \arg\min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

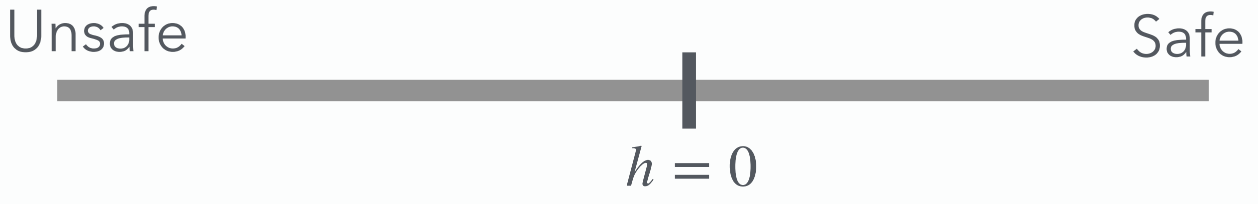
3. IN CLOSED FORM

A closed-form displacement

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

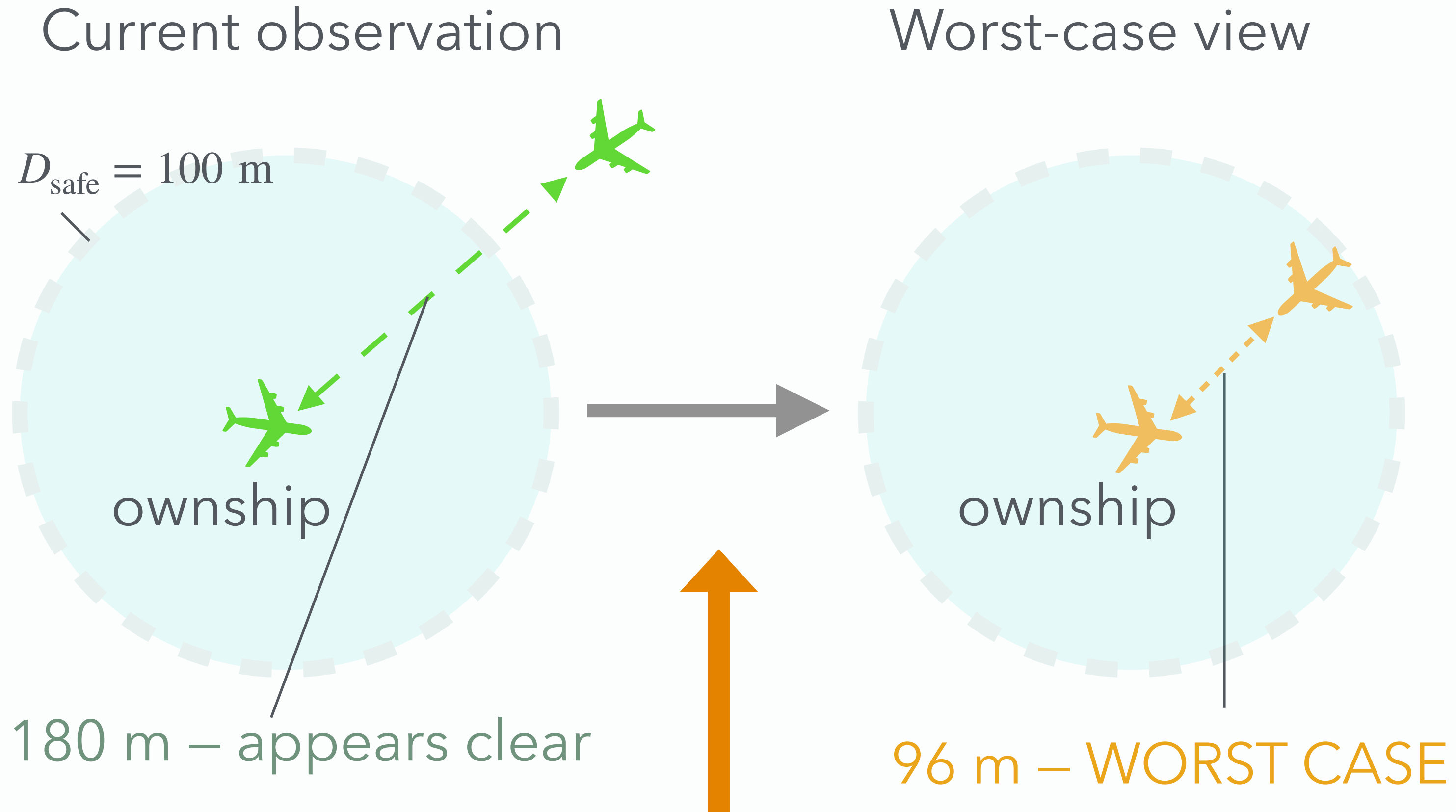
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

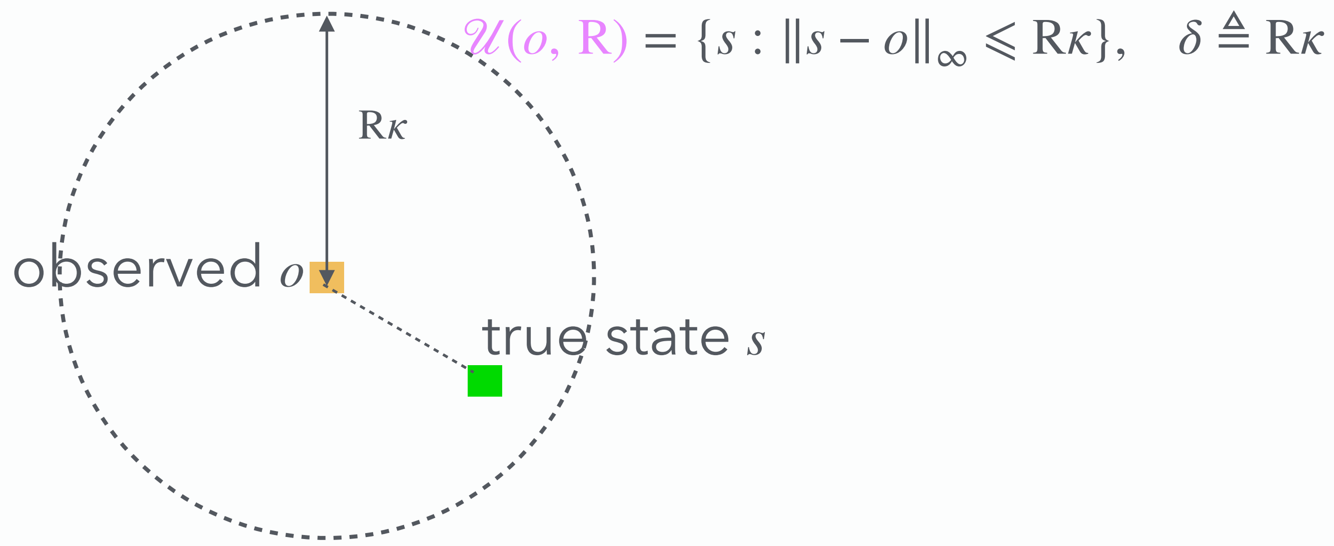
What looked clear now reads as a conflict



$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, R_{\max})} h(s)$$

3. IN CLOSED FORM

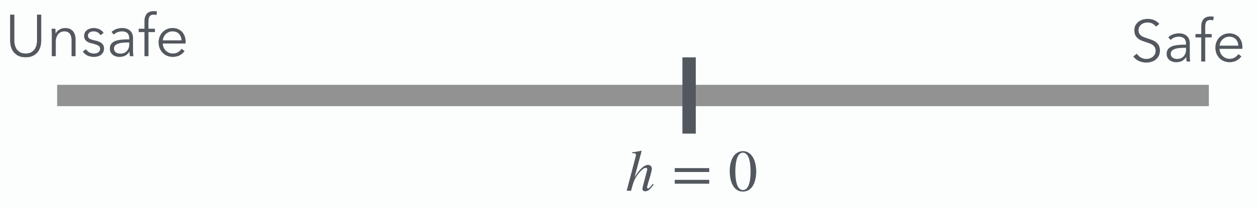
A closed-form displacement



Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

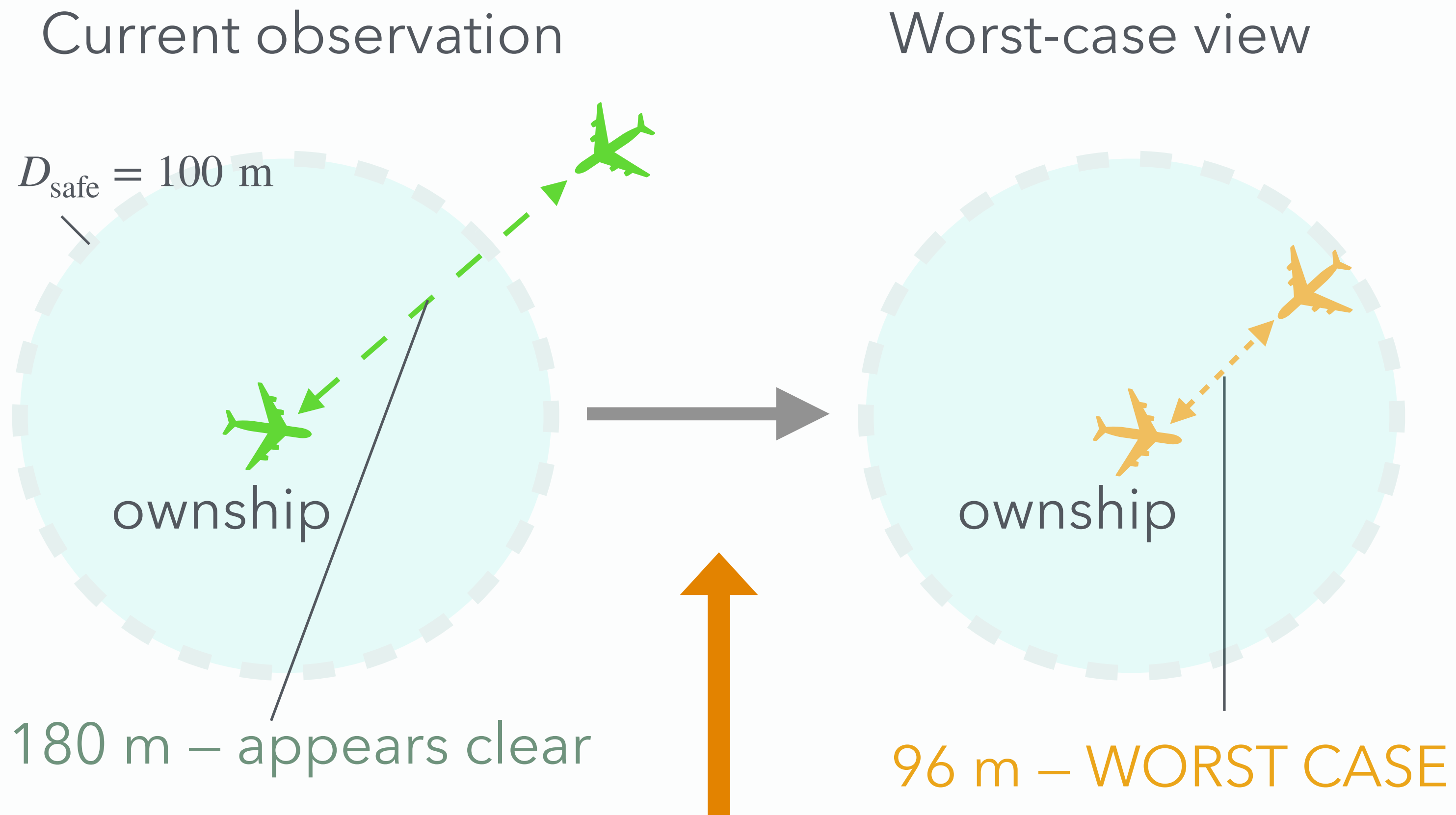
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

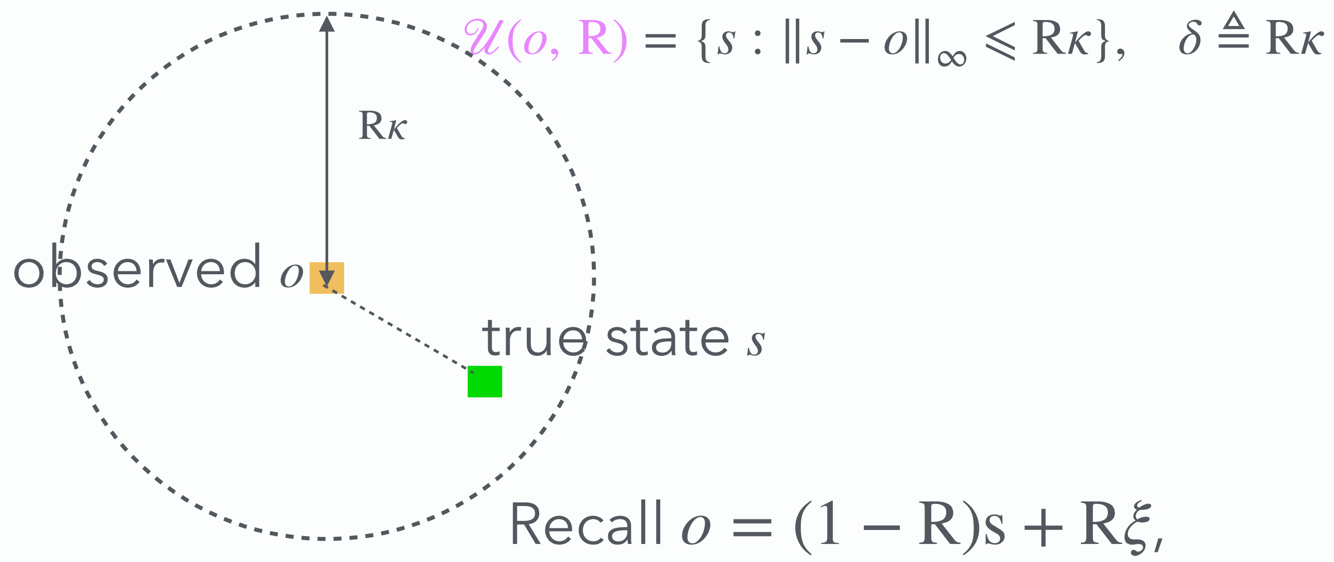
What looked clear now reads as a conflict



$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

3. IN CLOSED FORM

A closed-form displacement

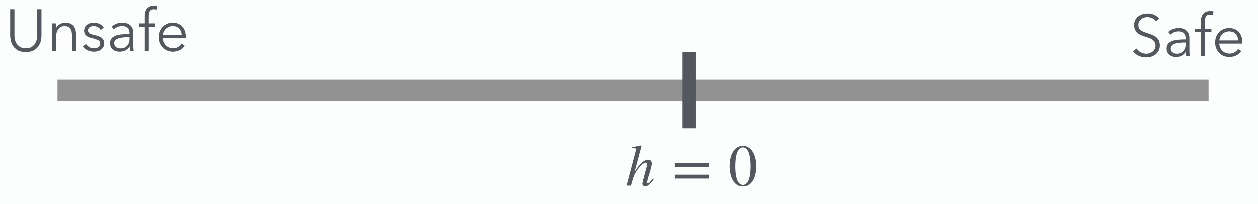


Recall $o = (1 - \mathrm{R})s + \mathrm{R}\xi$,
where $\|\xi - s\|_\infty \leqslant \kappa$

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

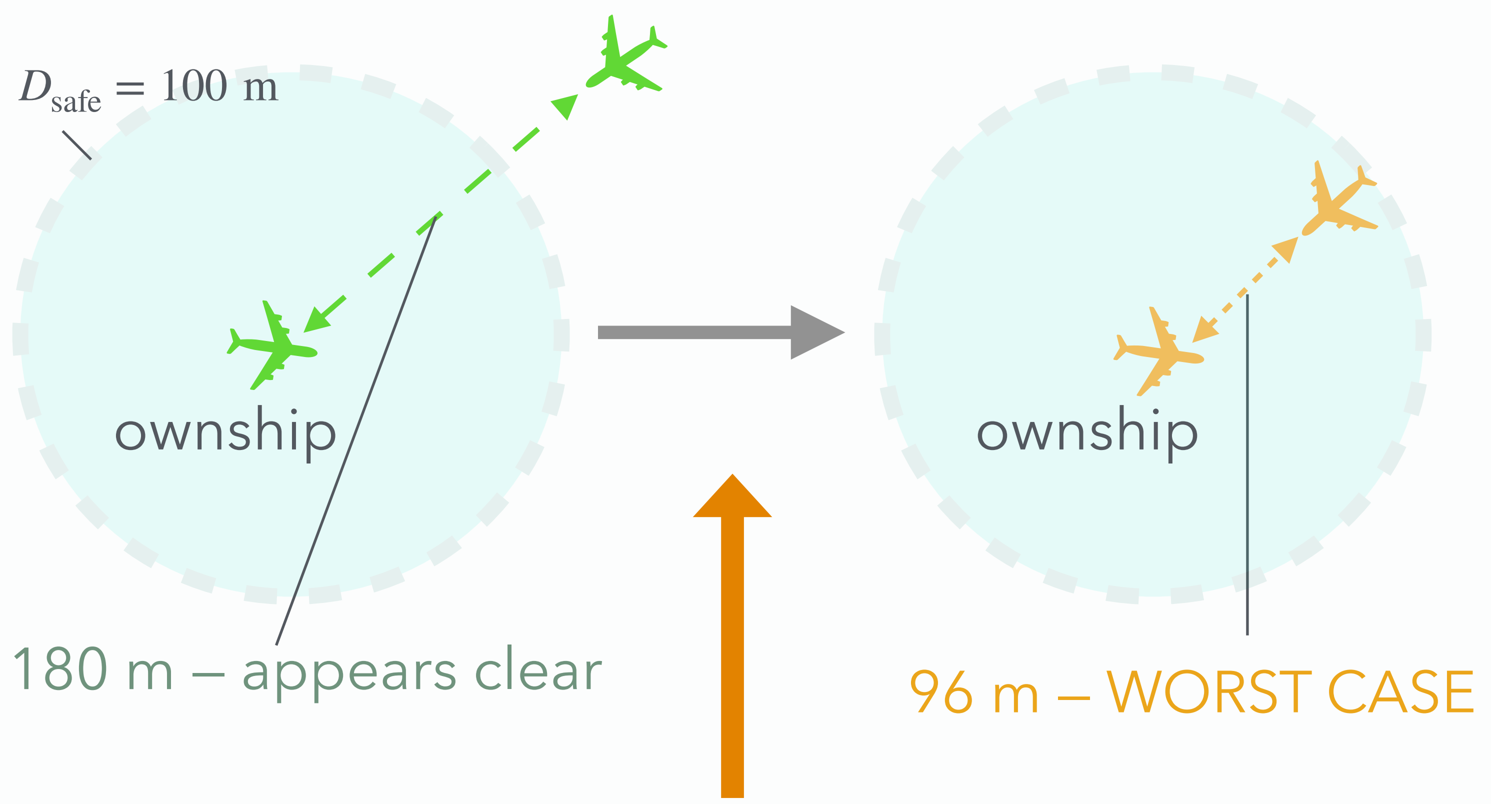
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

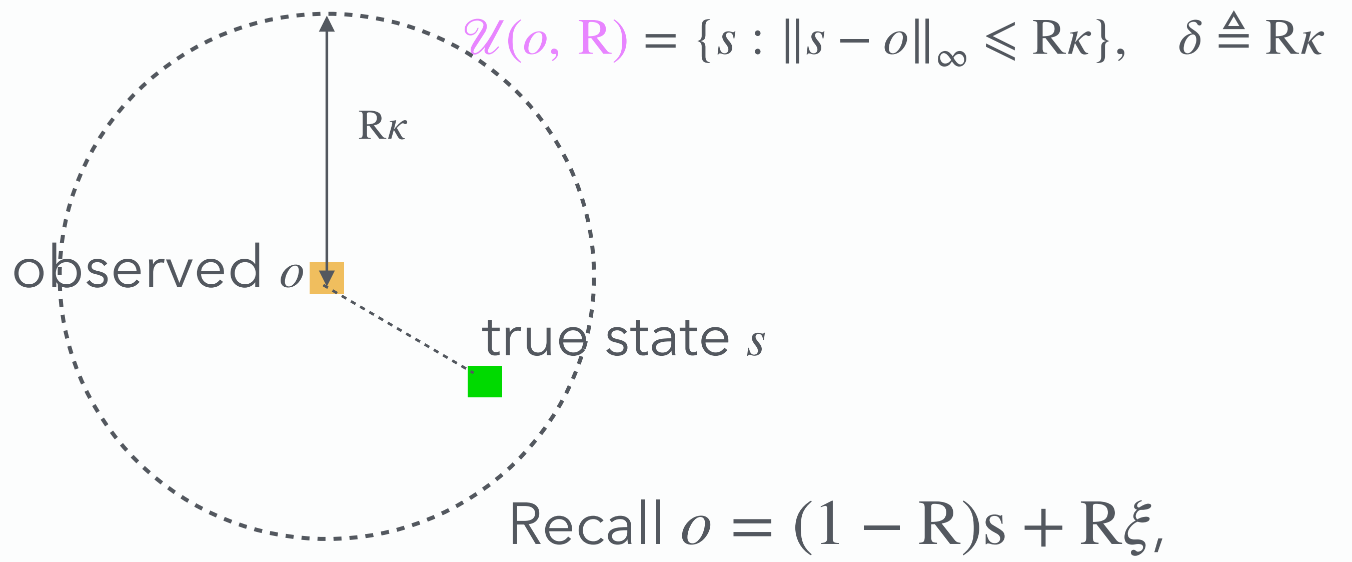
What looked clear now reads as a conflict



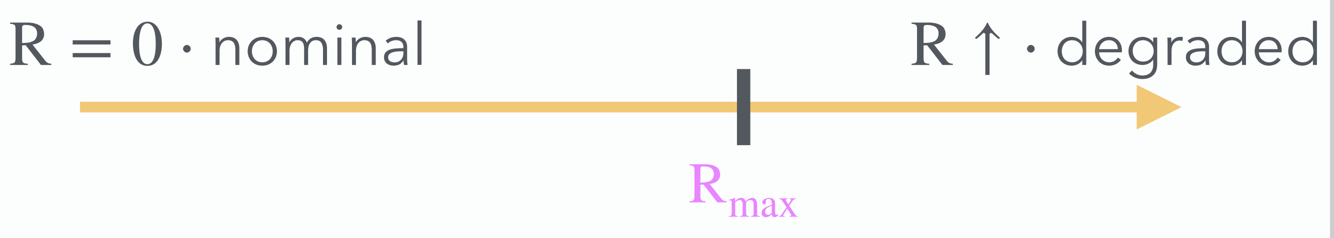
$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

3. IN CLOSED FORM

A closed-form displacement



Recall $o = (1 - \mathrm{R})s + \mathrm{R}\xi$,
where $\|\xi - s\|_\infty \leqslant \kappa$



03 APPROACH

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin

Unsafe — Safe

$h = 0$

$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

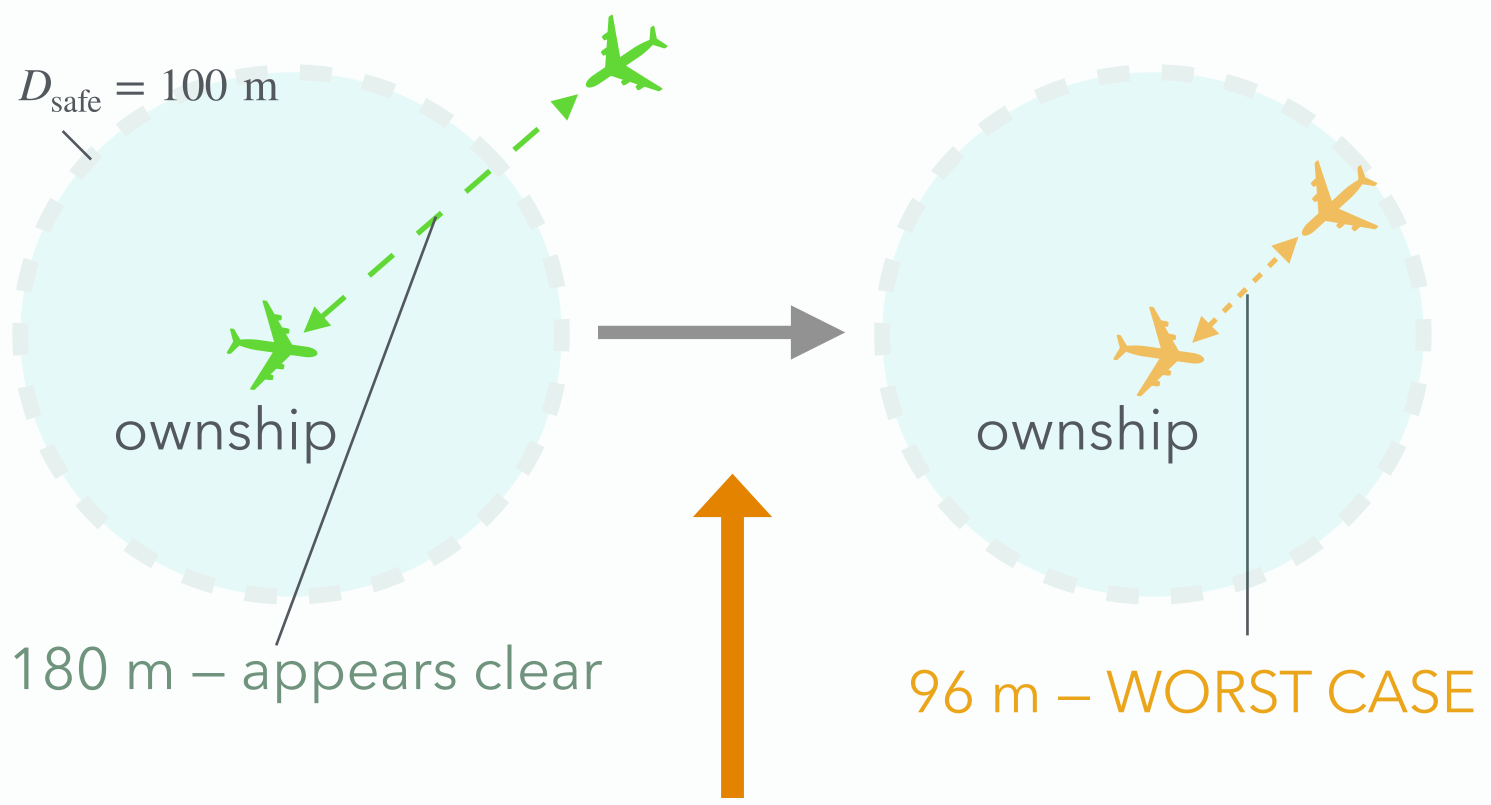
Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

What looked clear now reads as a conflict

Current observation

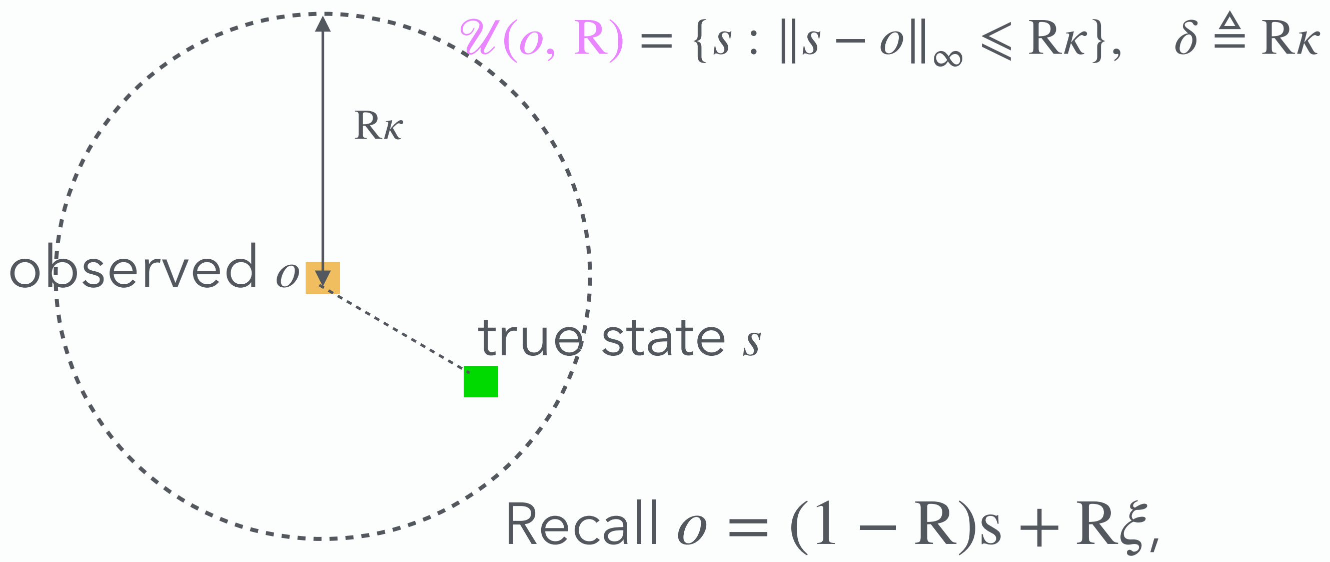
Worst-case view



$$s^\star = \arg\min_{s \in \mathcal{U}(o,\, \mathrm{R}_{\max})} h(s)$$

3. IN CLOSED FORM

A closed-form displacement



Recall $o = (1 - \mathrm{R})s + \mathrm{R}\xi$,
where $\|\xi - s\|_\infty \leqslant \kappa$

$\mathrm{R} = 0$ · nominal — $\mathrm{R} \uparrow$ · degraded

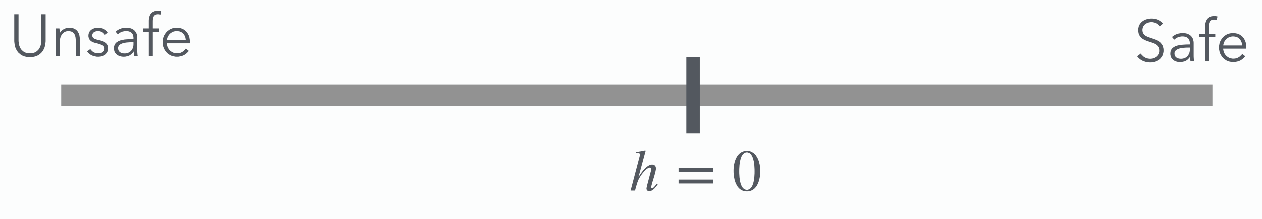
$\mathrm{R}_{\max}$

With $\mathrm{R}_{\max}$ as a design choice, $s^\star \leftarrow o \pm \mathrm{R}_{\max}\kappa$

Both filters start from the same worst-case state estimation

1. SAFETY MARGIN

Barrier function as safety margin



$$h(s) = (\|r\|^2 - D_{\text{safe}}^2) + \alpha \cdot r^T v_{\text{rel}}$$

$\|r\|^2 - D_{\text{safe}}^2$

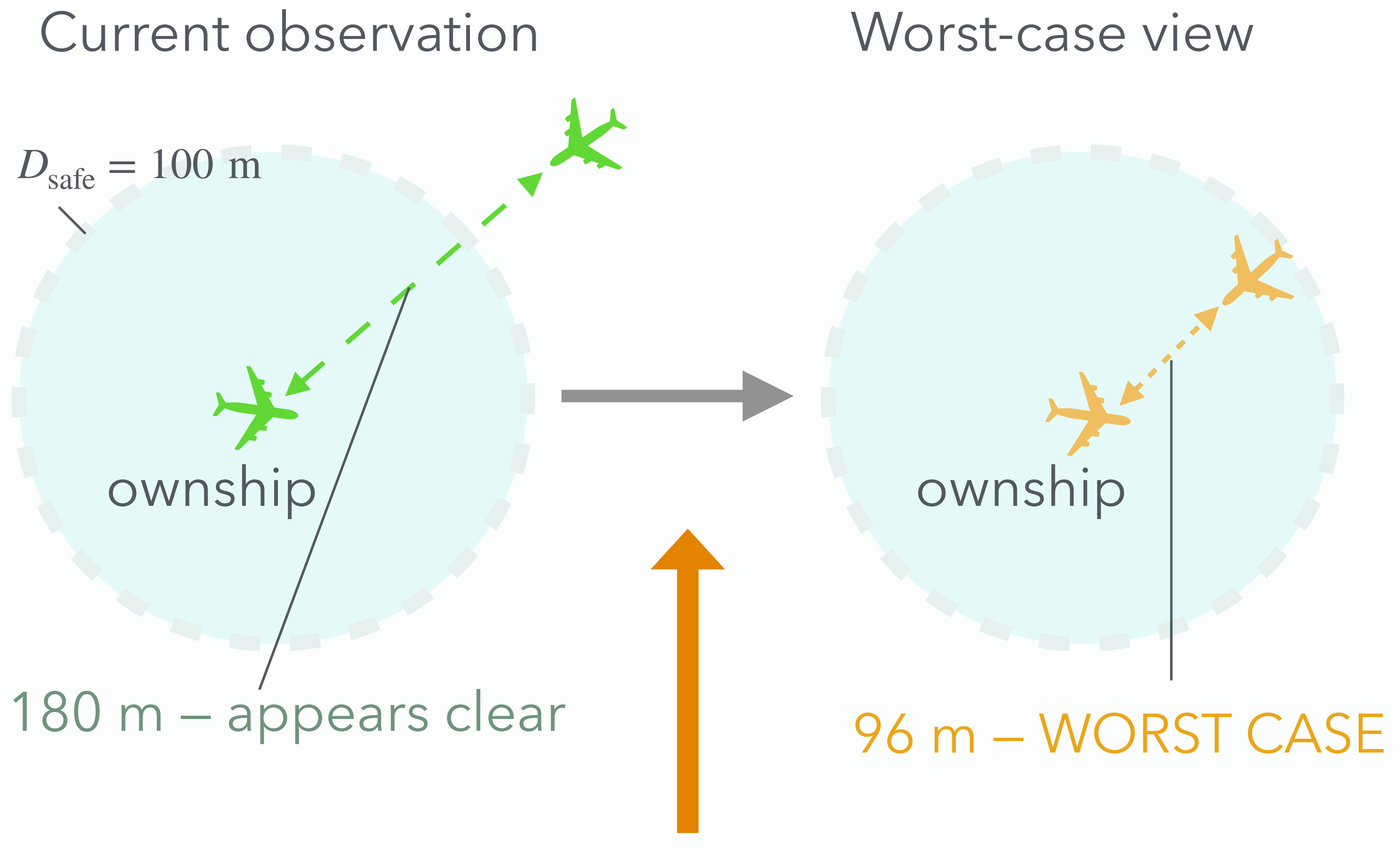
How much room there is between two UASs

$\alpha \cdot r^T v_{\text{rel}}$

Whether two UASs are closing in on each other
α sets how far ahead the margin looks

2. WORST CASE

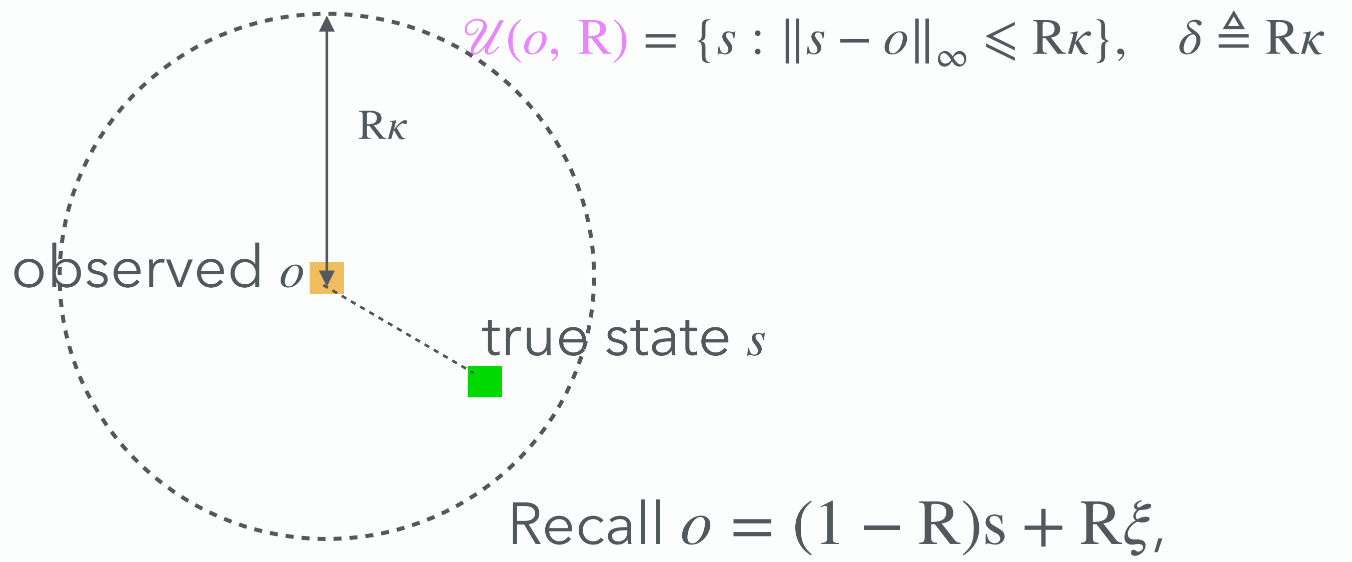
What looked clear now reads as a conflict



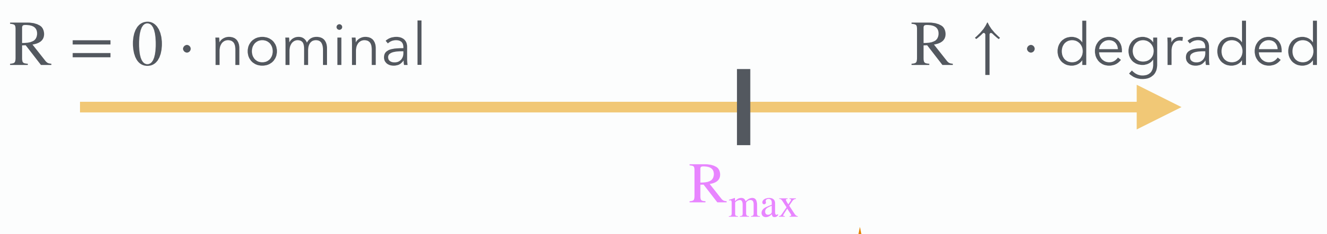
$$s^\star = \arg \min_{s \in \mathcal{U}(o,\, R_{\max})} h(s)$$

3. IN CLOSED FORM

A closed-form displacement



Recall $o = (1 - R)s + R\xi$,
where $\|\xi - s\|_\infty \leqslant \kappa$



With $R_{\max}$ as a design choice, $s^\star \leftarrow o \pm R_{\max}\kappa$

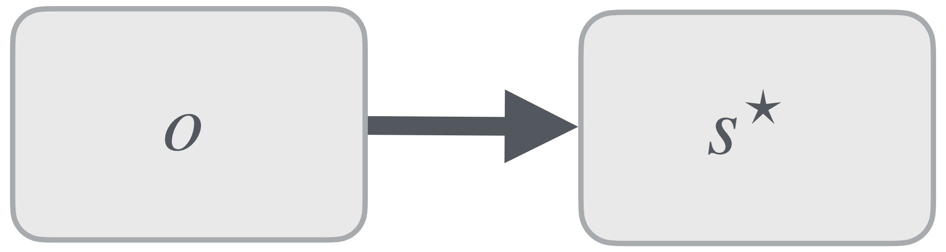
Both filters compute $s^\star$ from the same safety margin h. However, only the action filter lets h veto the policy.

The filtering approaches differ in what happens next

The filtering approaches differ in what happens next

o

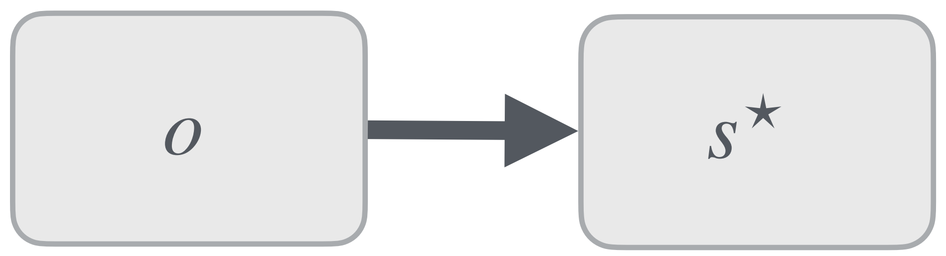
The filtering approaches differ in what happens next



shared worst-case state estimation

The filtering approaches differ in what happens next

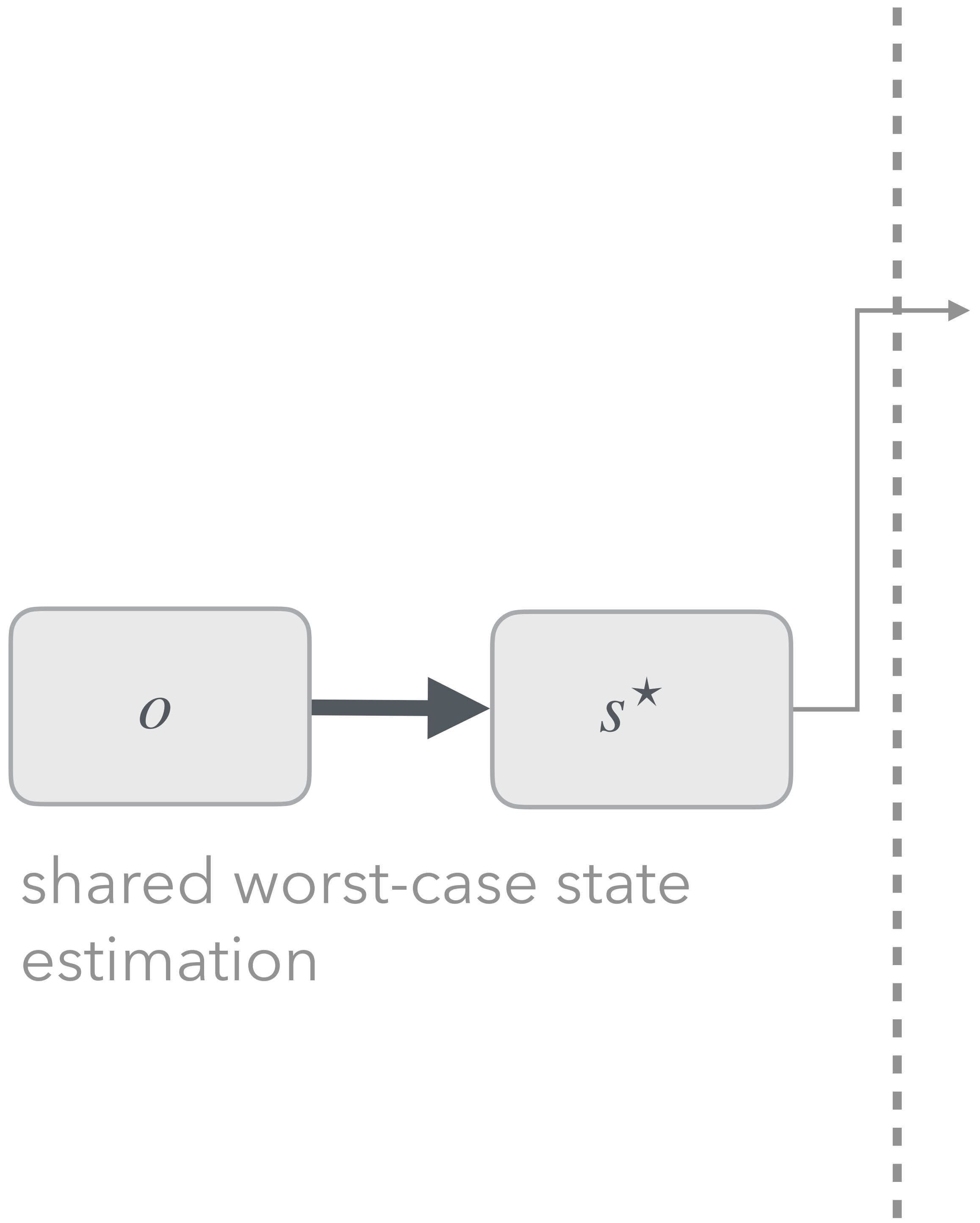
identical up to here



shared worst-case state estimation

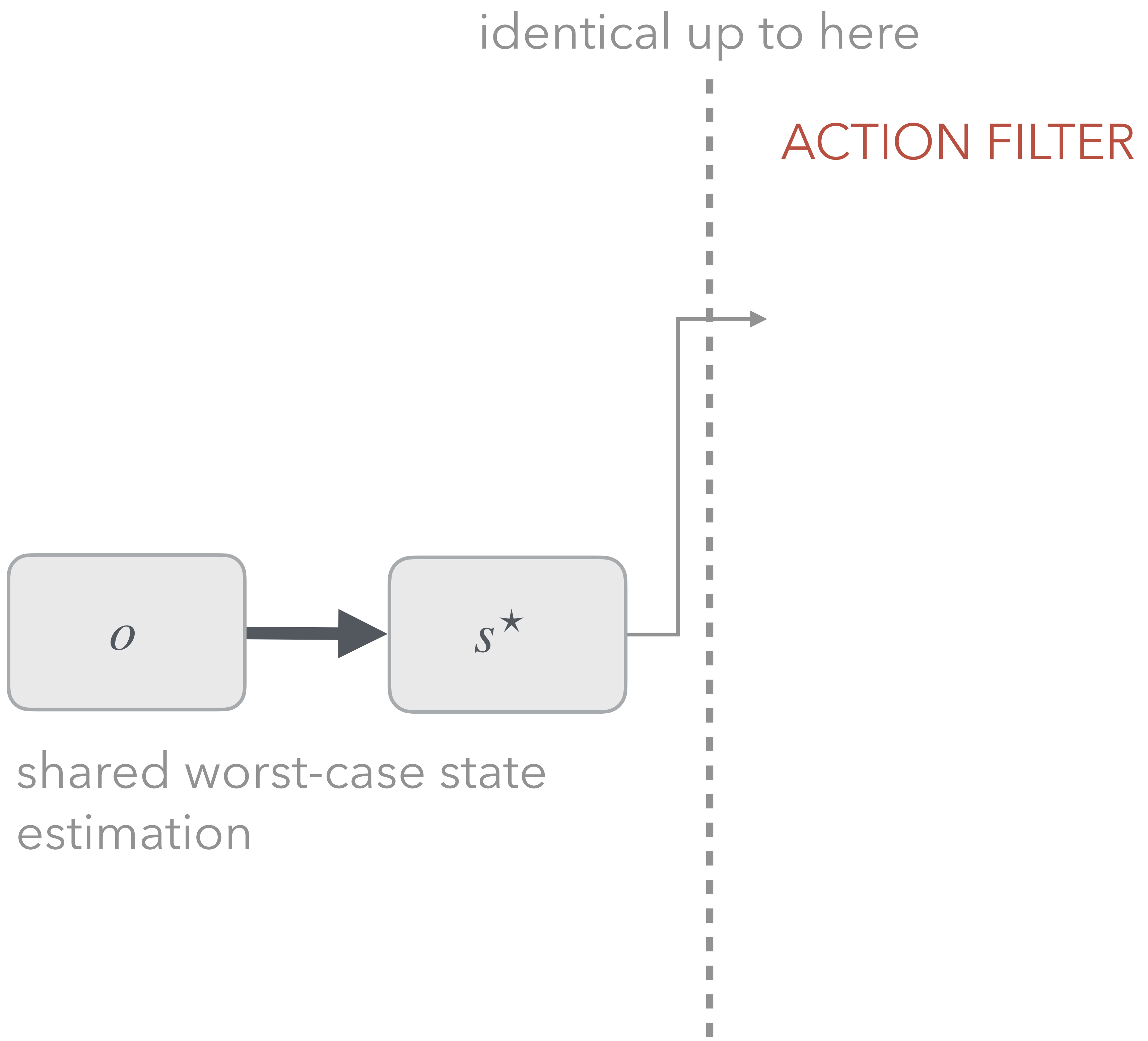
The filtering approaches differ in what happens next

identical up to here

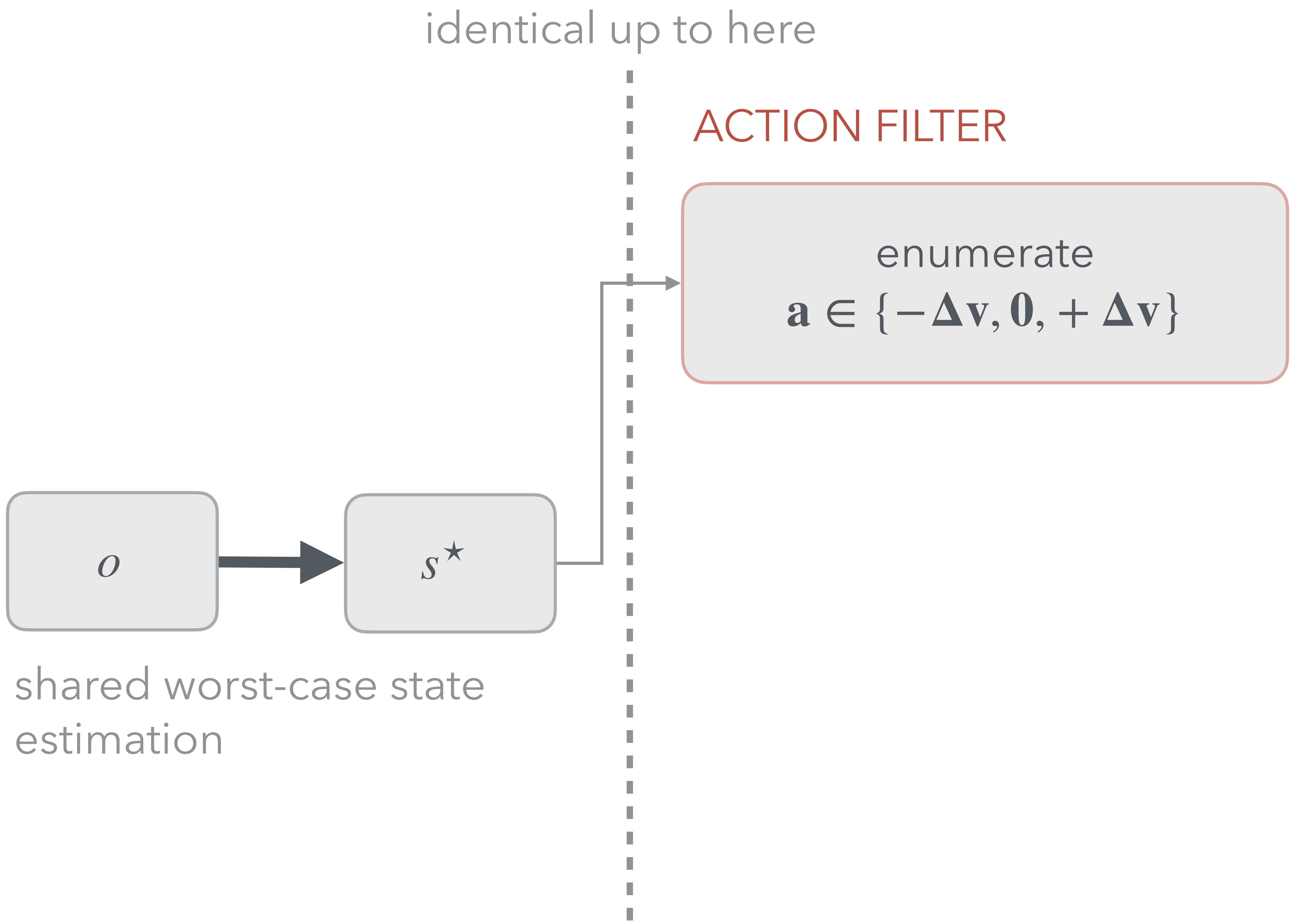


shared worst-case state estimation

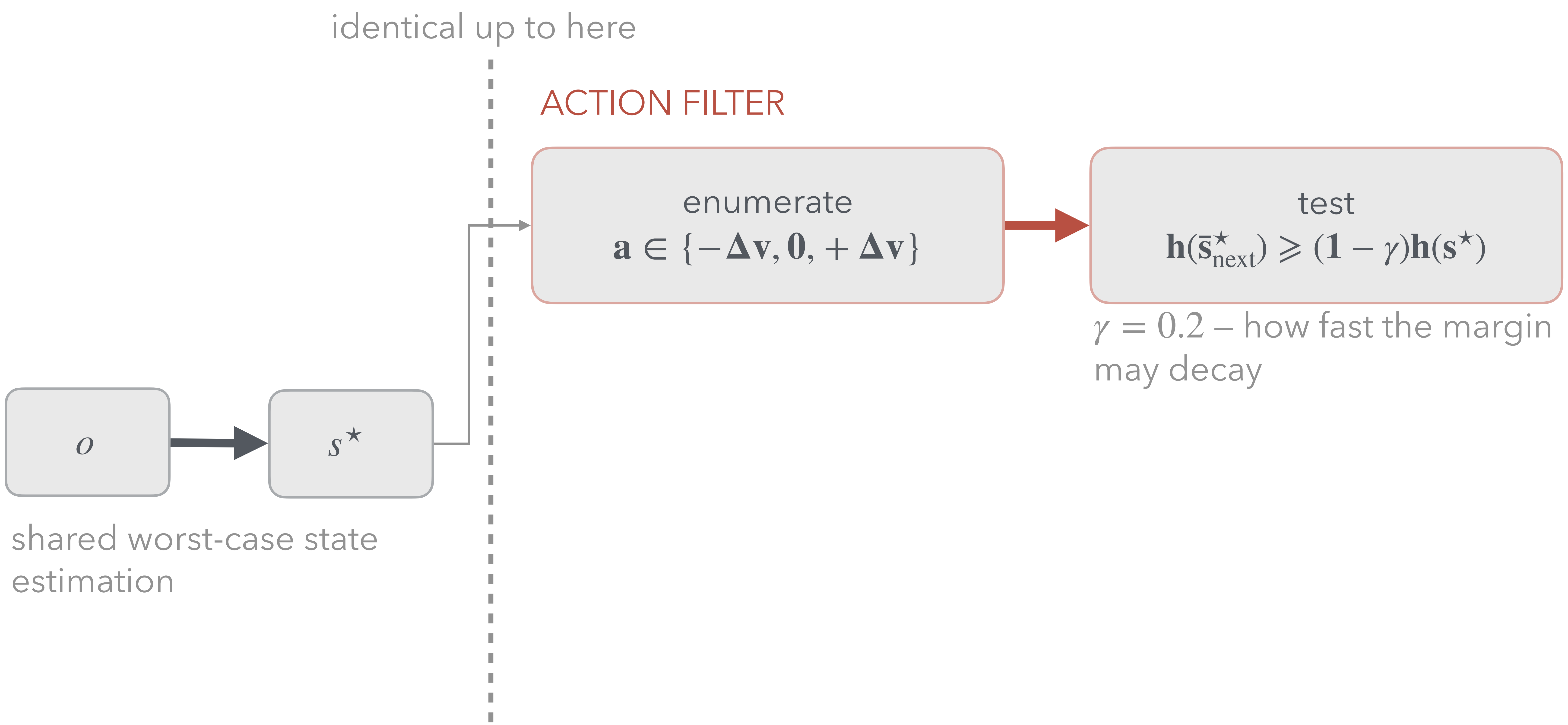
The filtering approaches differ in what happens next



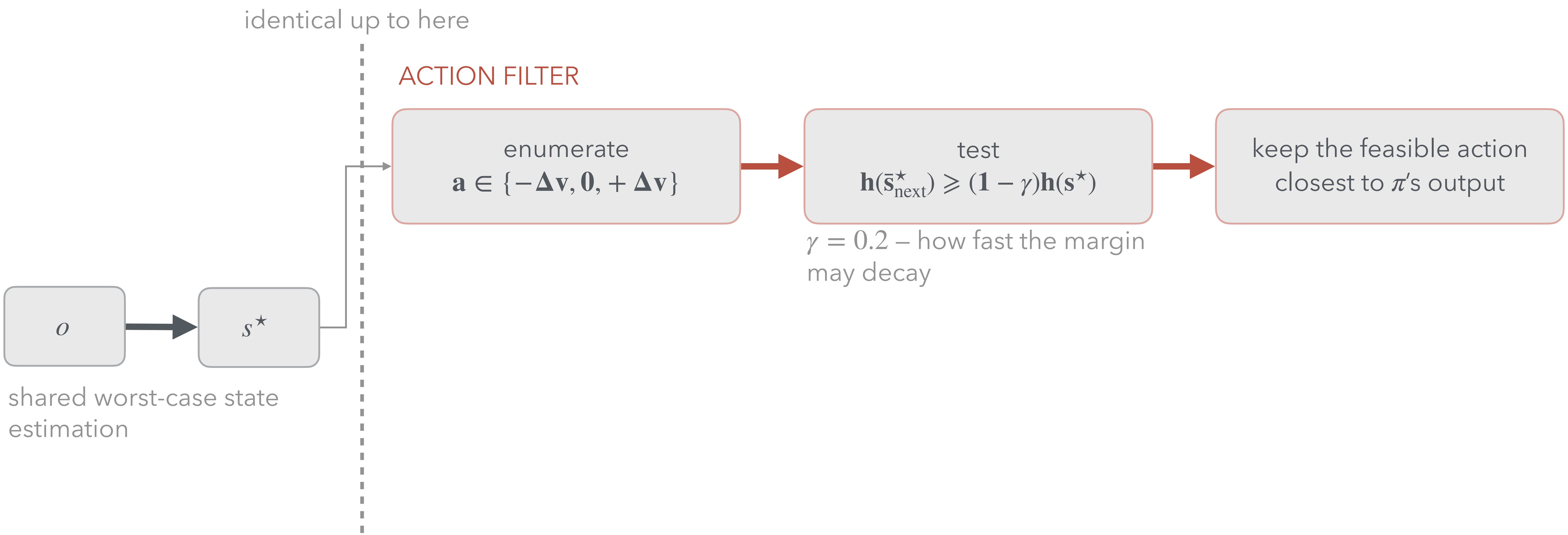
The filtering approaches differ in what happens next



The filtering approaches differ in what happens next



The filtering approaches differ in what happens next



The filtering approaches differ in what happens next

identical up to here

ACTION FILTER

enumerate
$\mathbf{a} \in \{-\Delta\mathbf{v}, \mathbf{0}, +\Delta\mathbf{v}\}$

test
$\mathbf{h}(\bar{\mathbf{s}}^{\star}_{\text{next}}) \geqslant (\mathbf{1}-\gamma)\mathbf{h}(\mathbf{s}^{\star})$

keep the feasible action closest to π's output

$\gamma = 0.2$ – how fast the margin may decay

o

$s^{\star}$

shared worst-case state estimation

The filtering approaches differ in what happens next

identical up to here

ACTION FILTER

enumerate
$\mathbf{a} \in \{-\Delta \mathbf{v}, \mathbf{0}, +\Delta \mathbf{v}\}$

test
$\mathbf{h}(\bar{\mathbf{s}}^\star_{\text{next}}) \geqslant (\mathbf{1}-\gamma)\mathbf{h}(\mathbf{s}^\star)$

$\gamma = 0.2$ – how fast the margin may decay

keep the feasible action closest to π's output

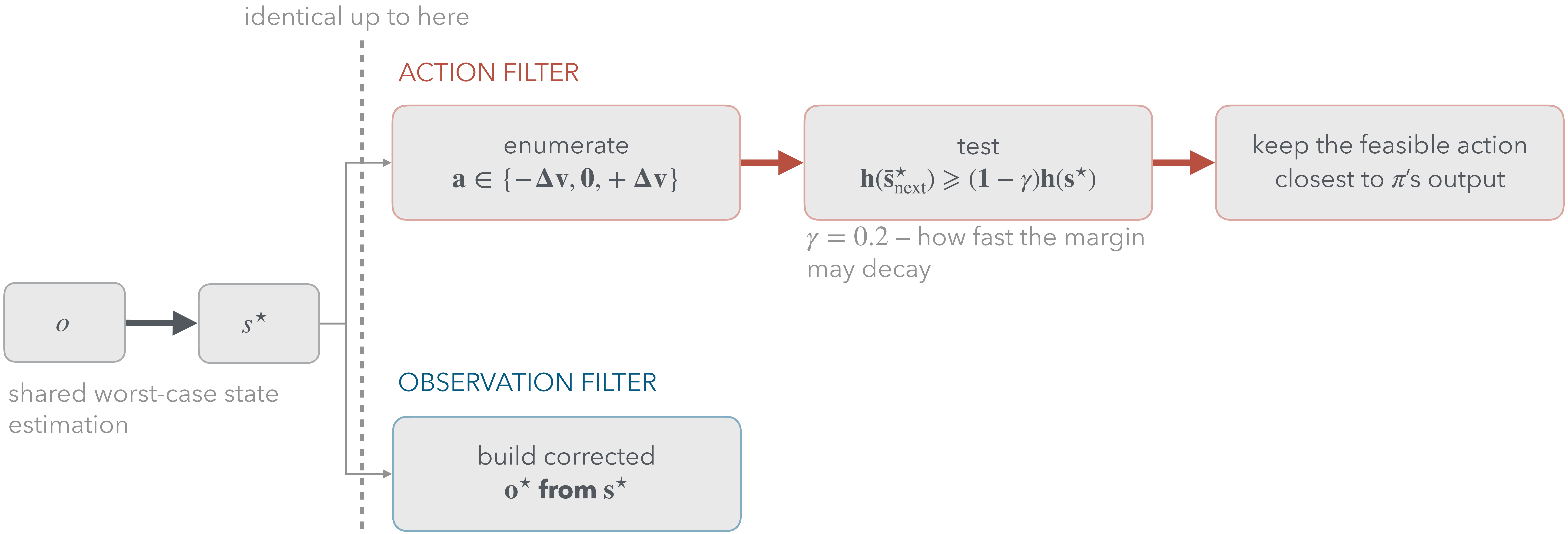
o

$s^\star$

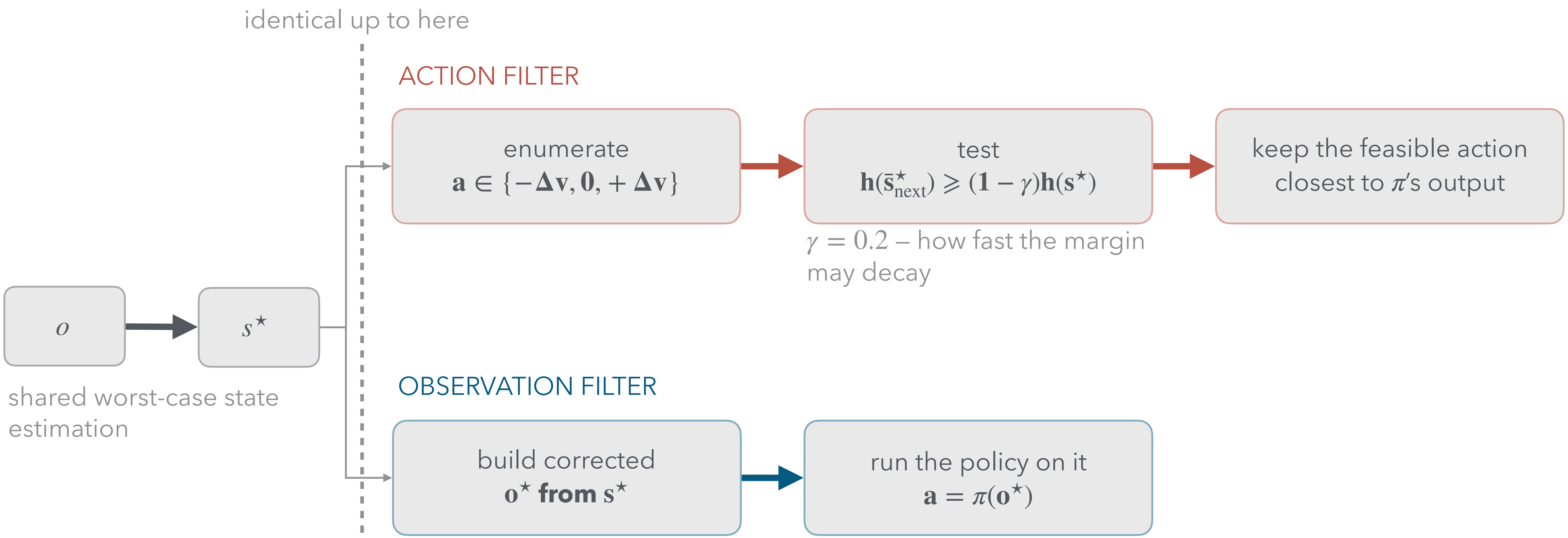
shared worst-case state estimation

OBSERVATION FILTER

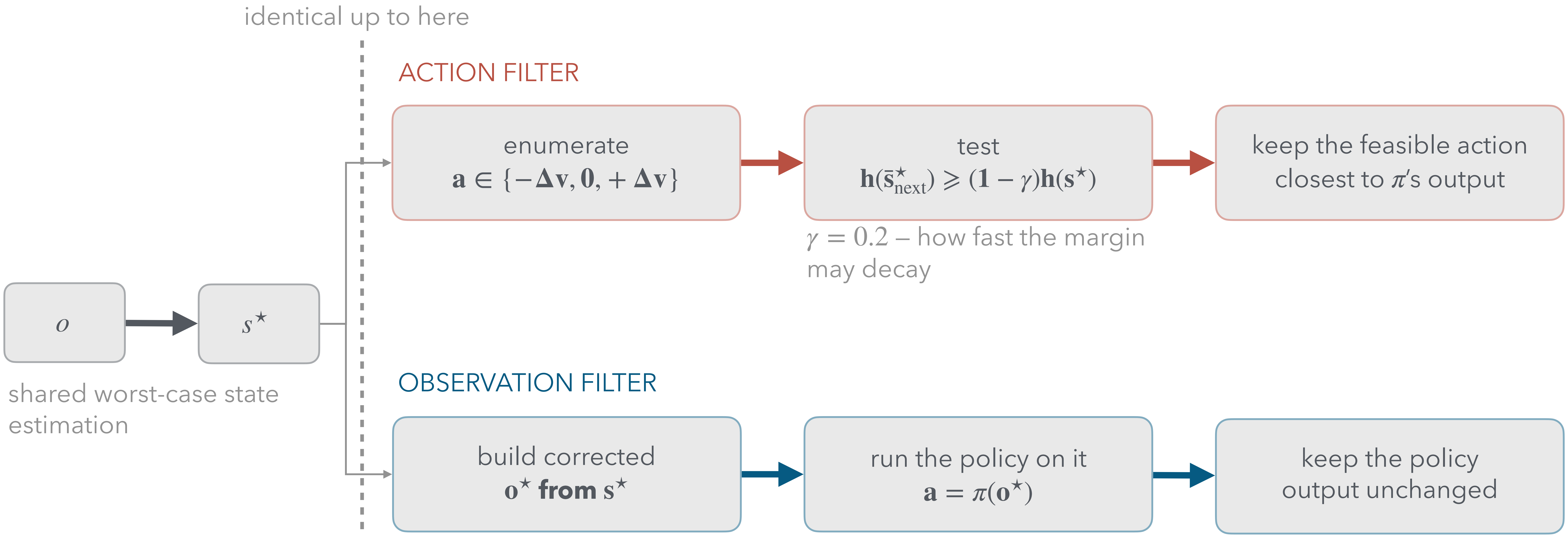
The filtering approaches differ in what happens next



The filtering approaches differ in what happens next



The filtering approaches differ in what happens next



The filtering approaches differ in what happens next

identical up to here

o → $s^\star$

shared worst-case state estimation

ACTION FILTER

enumerate $\mathbf{a} \in \{-\Delta \mathbf{v}, \mathbf{0}, +\Delta \mathbf{v}\}$ → test $\mathbf{h}(\bar{\mathbf{s}}^\star_{\text{next}}) \geqslant (\mathbf{1}-\gamma)\mathbf{h}(\mathbf{s}^\star)$ → keep the feasible action closest to π's output

$\gamma = 0.2$ – how fast the margin may decay

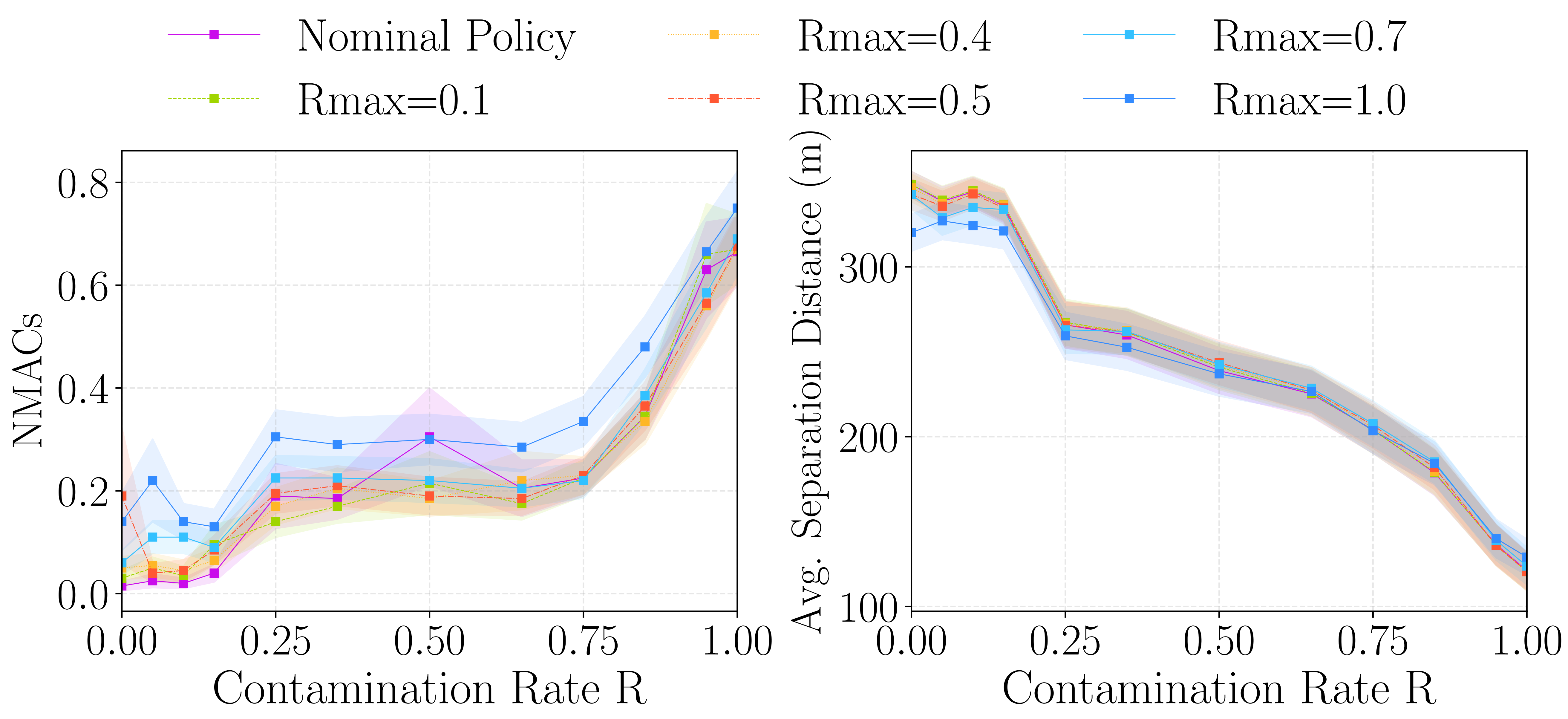
OBSERVATION FILTER

build corrected $\mathbf{o}^\star$ **from** $\mathbf{s}^\star$ → run the policy on it $\mathbf{a} = \pi(\mathbf{o}^\star)$ → keep the policy output unchanged

Same estimate, different use. The discrete-time CBF condition applies only to the action filtering.

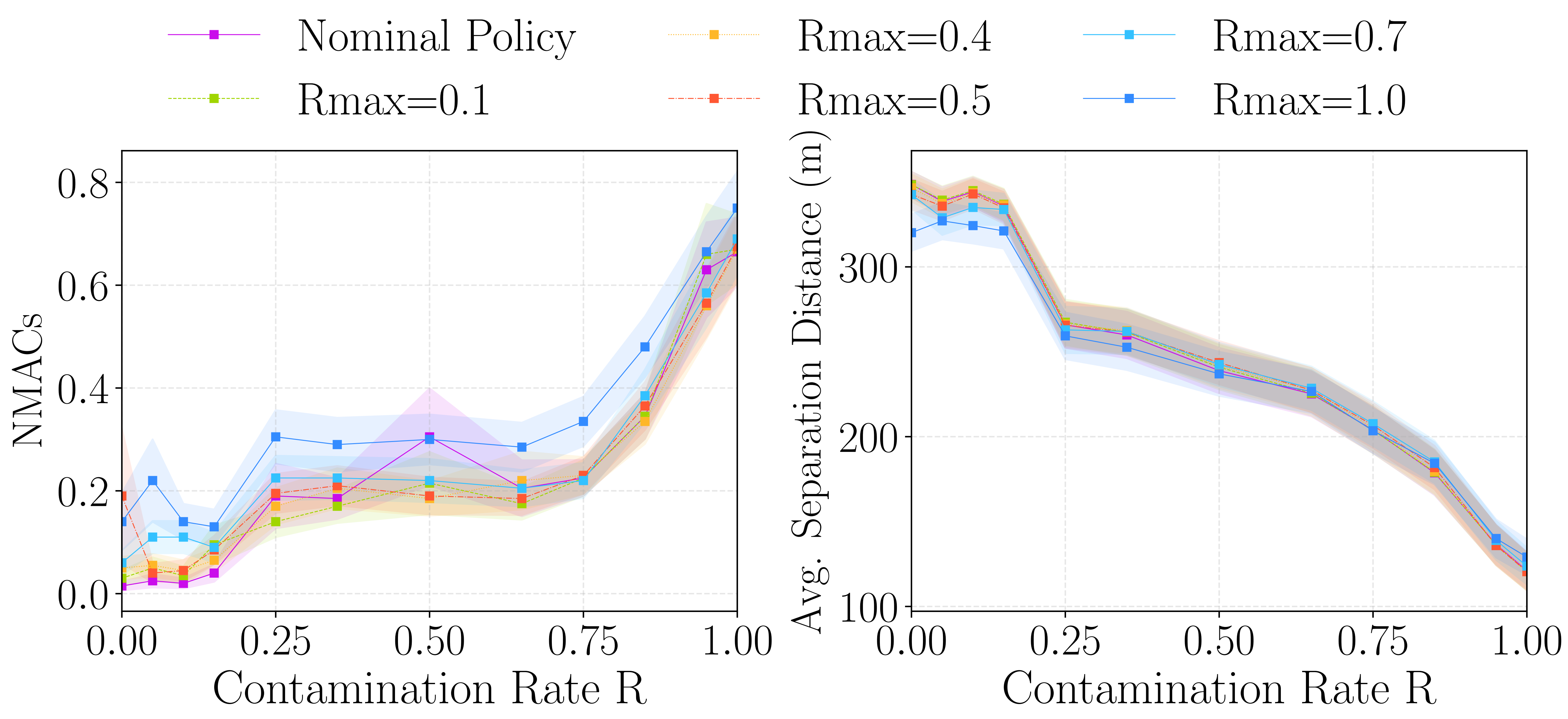
Action filtering barely moves the safety needle

Action filtering barely moves the safety needle



Shaded bands are ± standard error.

Action filtering barely moves the safety needle

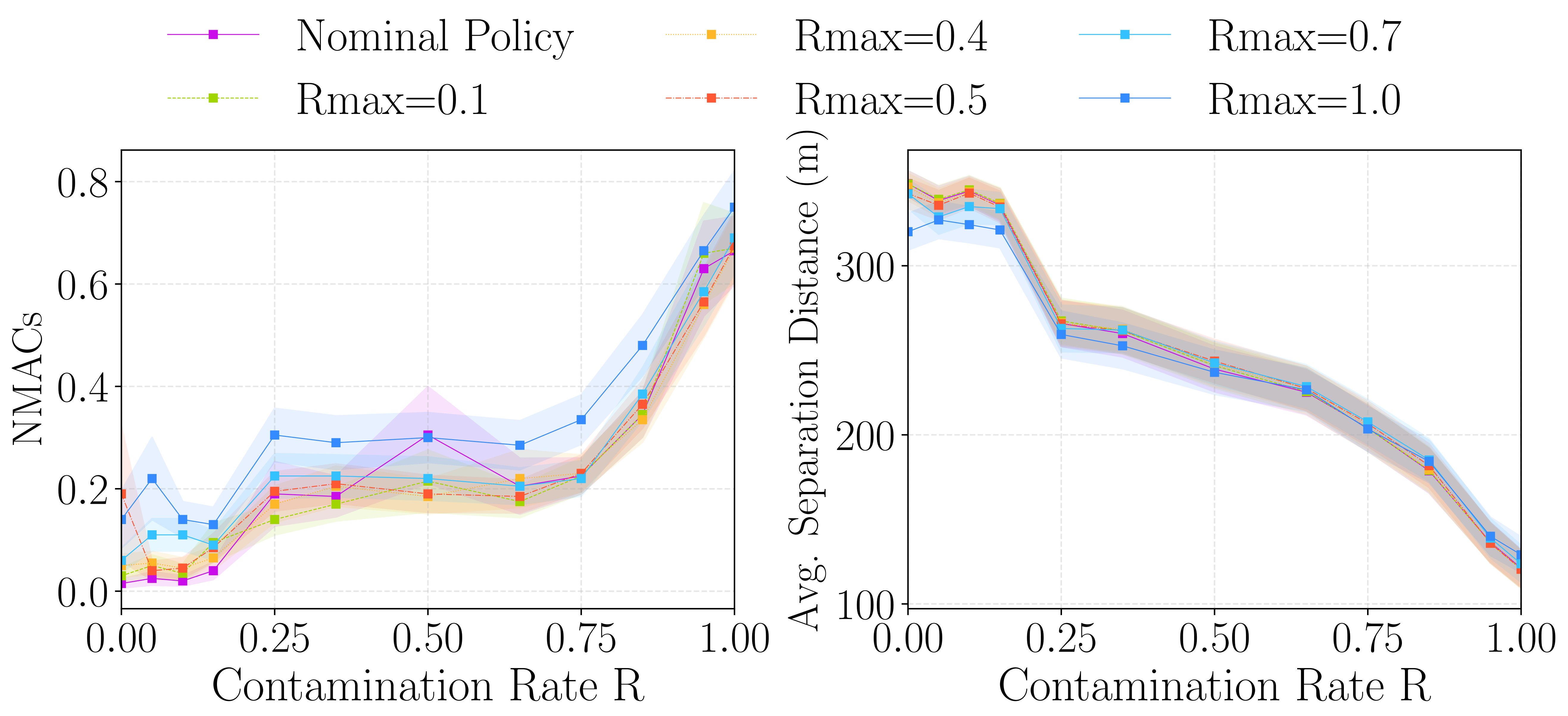


Shaded bands are ± standard error.

Action filtering barely moves the safety needle

NMAC

Near mid-air collision when two aircraft pass within $D_{\text{safe}} = 100$ m; counted per episode.



Shaded bands are ± standard error.

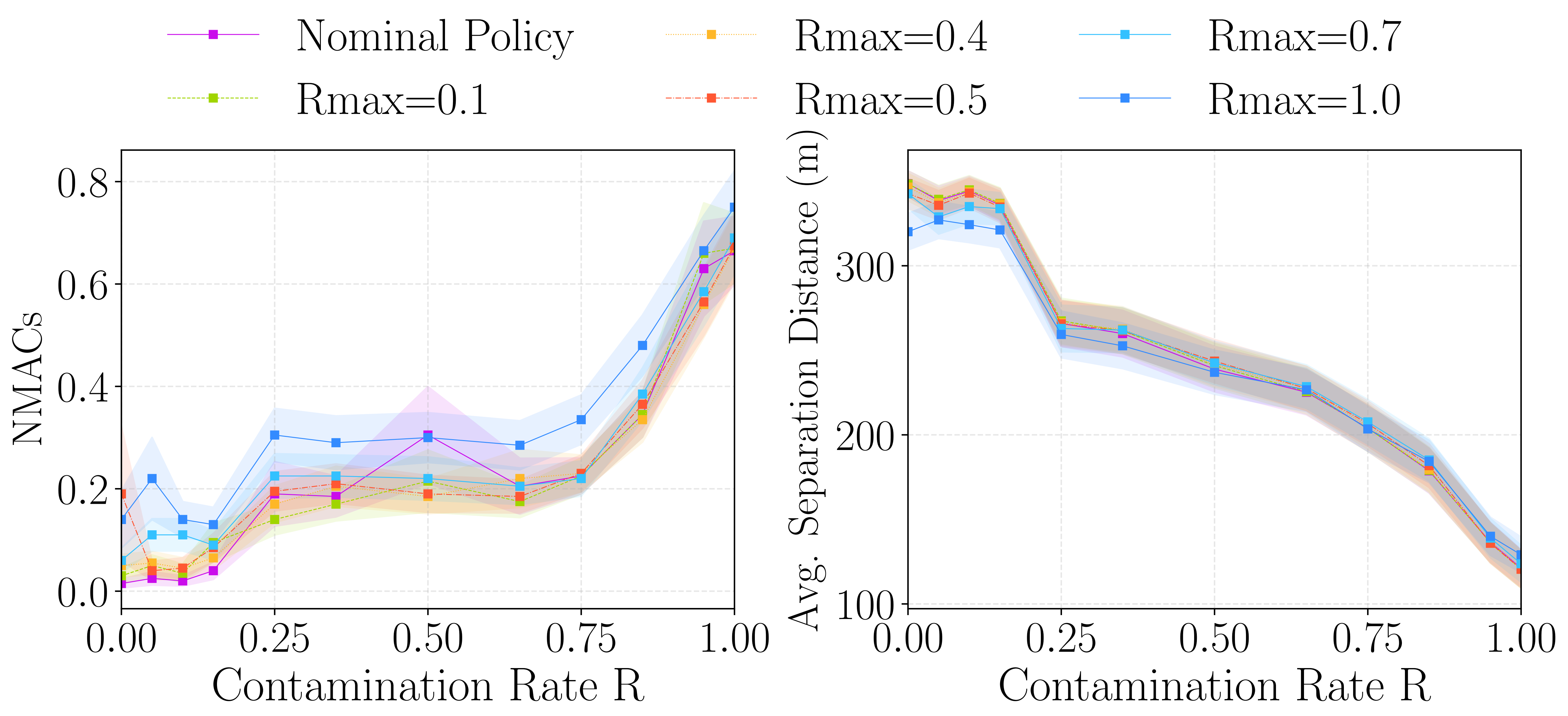
Action filtering barely moves the safety needle

NMAC

Near mid-air collision when two aircraft pass within $D_{\text{safe}} = 100$ m; counted per episode.

R

Contamination rate: how degraded GNSS actually is. 0 is nominal; 1 is fully adversarial.



Shaded bands are ± standard error.

Action filtering barely moves the safety needle

NMAC

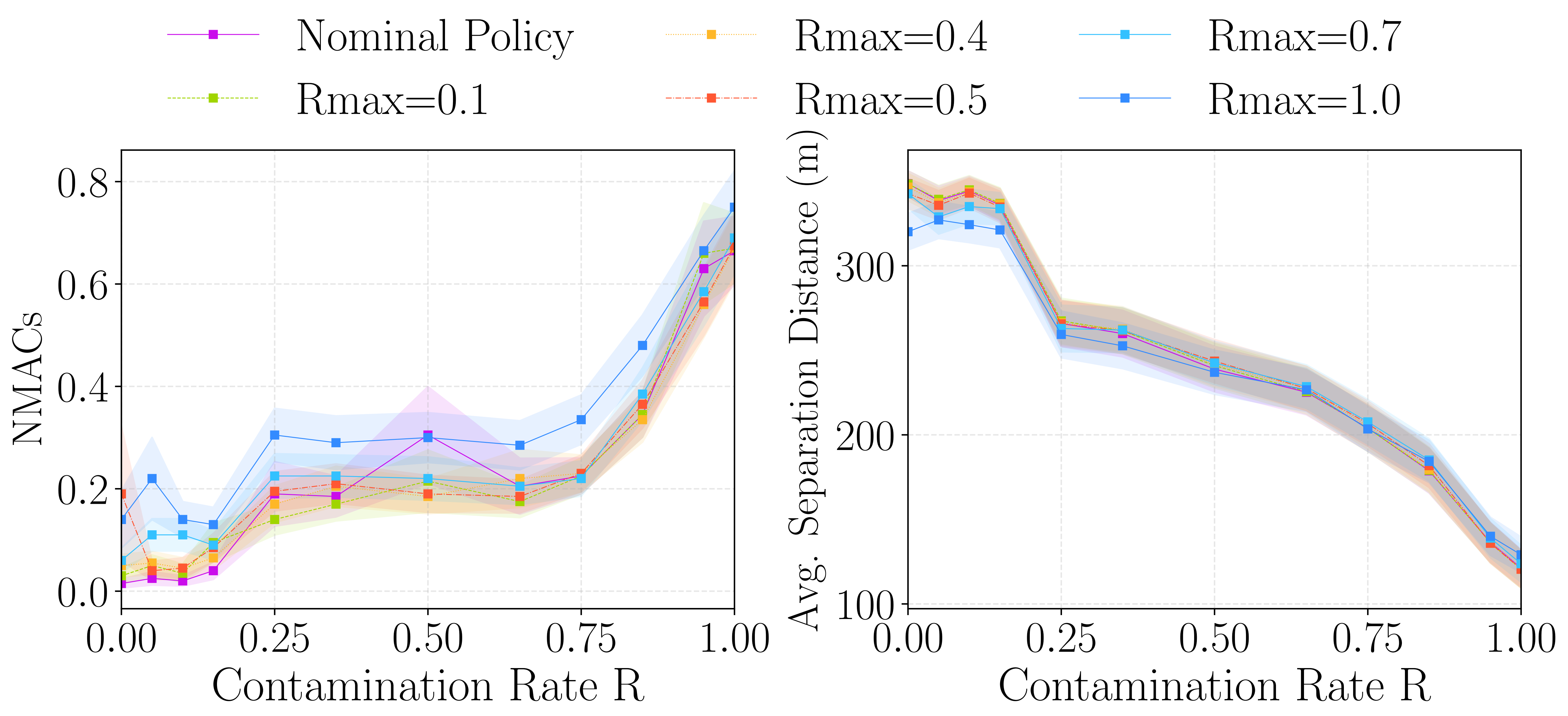
Near mid-air collision when two aircraft pass within $D_{\text{safe}} = 100$ m; counted per episode.

R

Contamination rate: how degraded GNSS actually is. 0 is nominal; 1 is fully adversarial.

R_{max}

What the filter assumes: a design choice fixed before deployment.



Shaded bands are ± standard error.

Action filtering barely moves the safety needle

NMAC

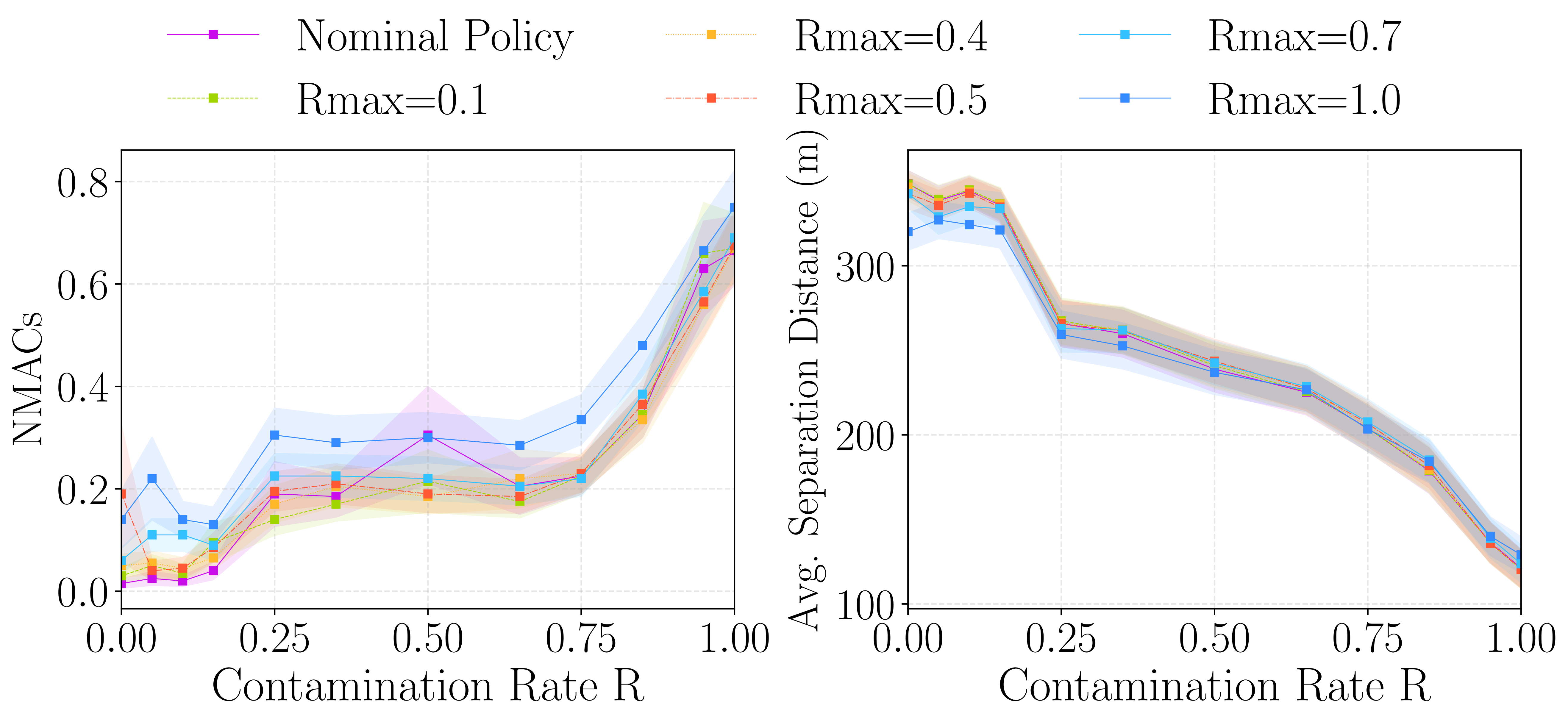
Near mid-air collision when two aircraft pass within $D_{\text{safe}} = 100$ m; counted per episode.

R

Contamination rate: how degraded GNSS actually is. 0 is nominal; 1 is fully adversarial.

$\mathrm{R}_{\max}$

What the filter assumes: a design choice fixed before deployment.

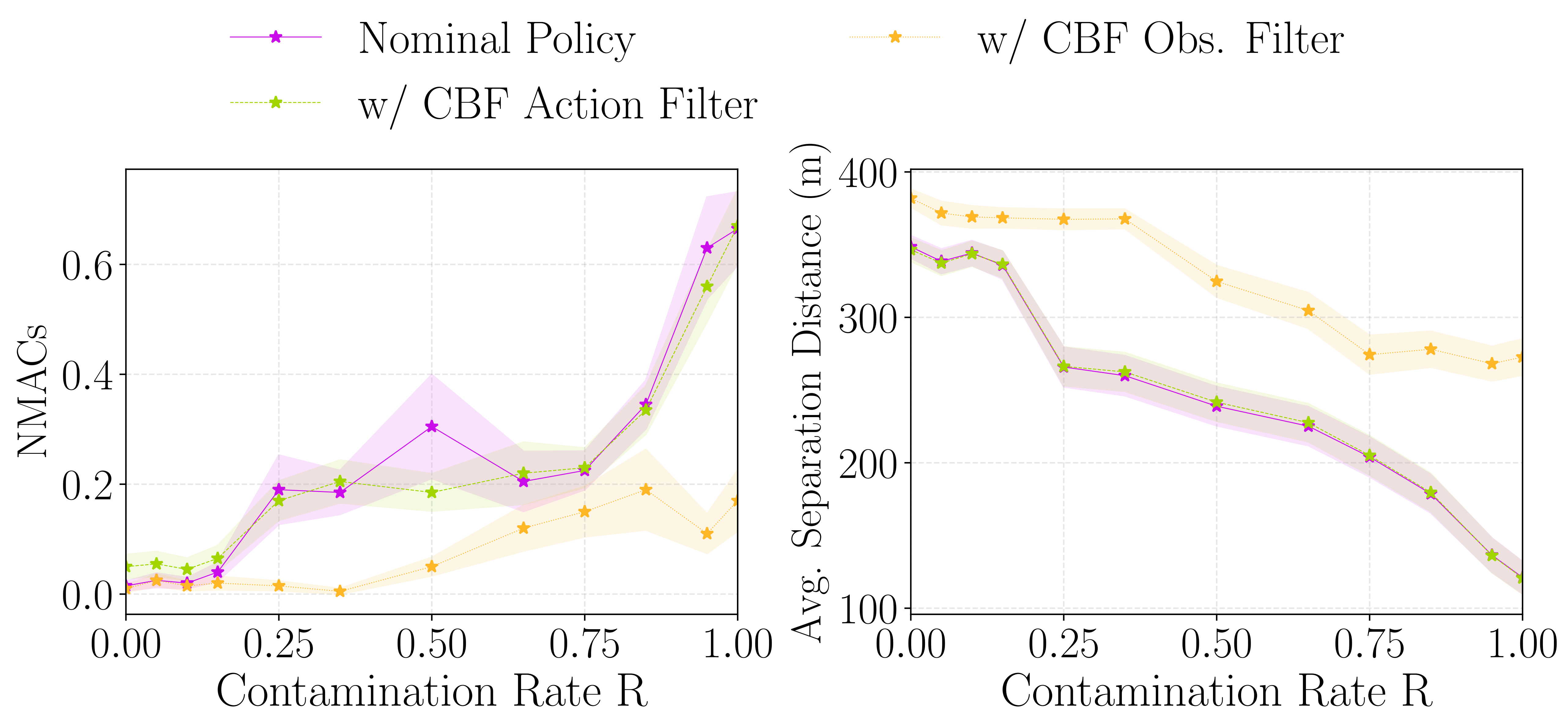


Shaded bands are ± standard error.

Every setting tracks the nominal policy. Despite changing $\mathrm{R}_{\max}$, action filtering does not separate from the unfiltered baseline.

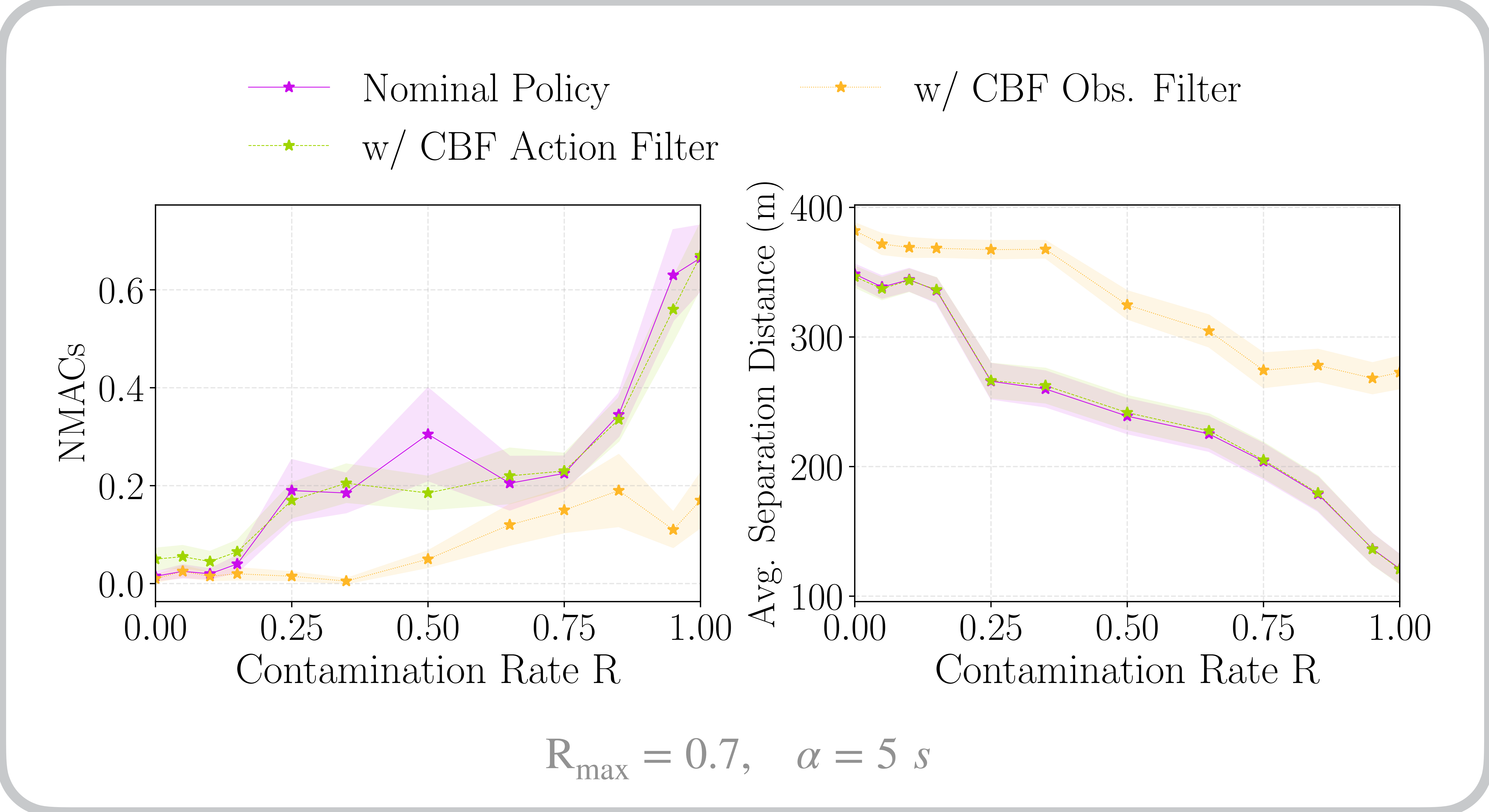
Observation filtering removes nine near collisions in ten

Observation filtering removes nine near collisions in ten



$R_{max} = 0.7, \quad \alpha = 5\ s$

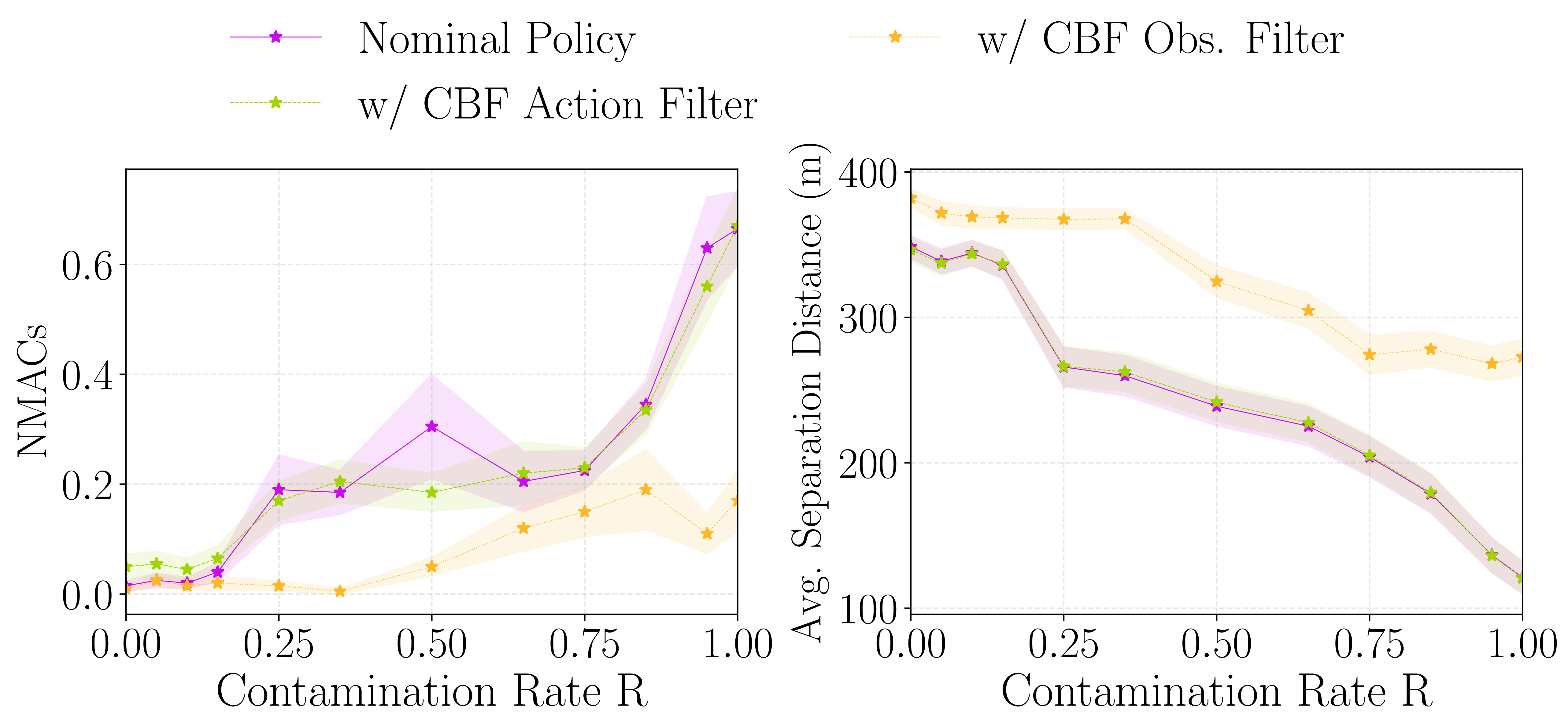
Observation filtering removes nine near collisions in ten



Observation filtering removes nine near collisions in ten

90%

fewer near mid-air collisions



$R_{max} = 0.7, \quad \alpha = 5\ s$

04 RESULTS

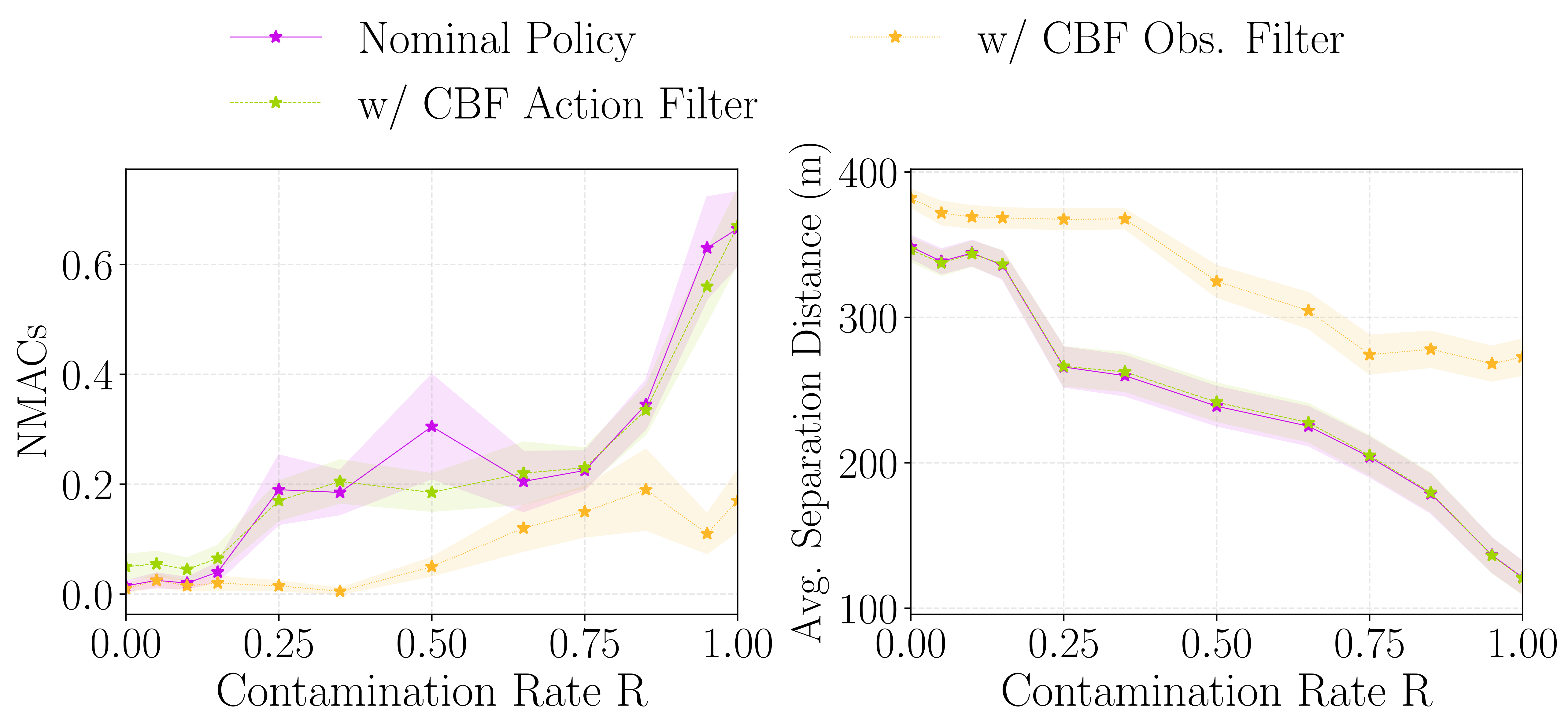
Observation filtering removes nine near collisions in ten

90%

fewer near mid-air collisions

0.24 → 0.02

NMACs per episode



$R_{max} = 0.7, \quad \alpha = 5\ s$

Observation filtering removes nine near collisions in ten

90%

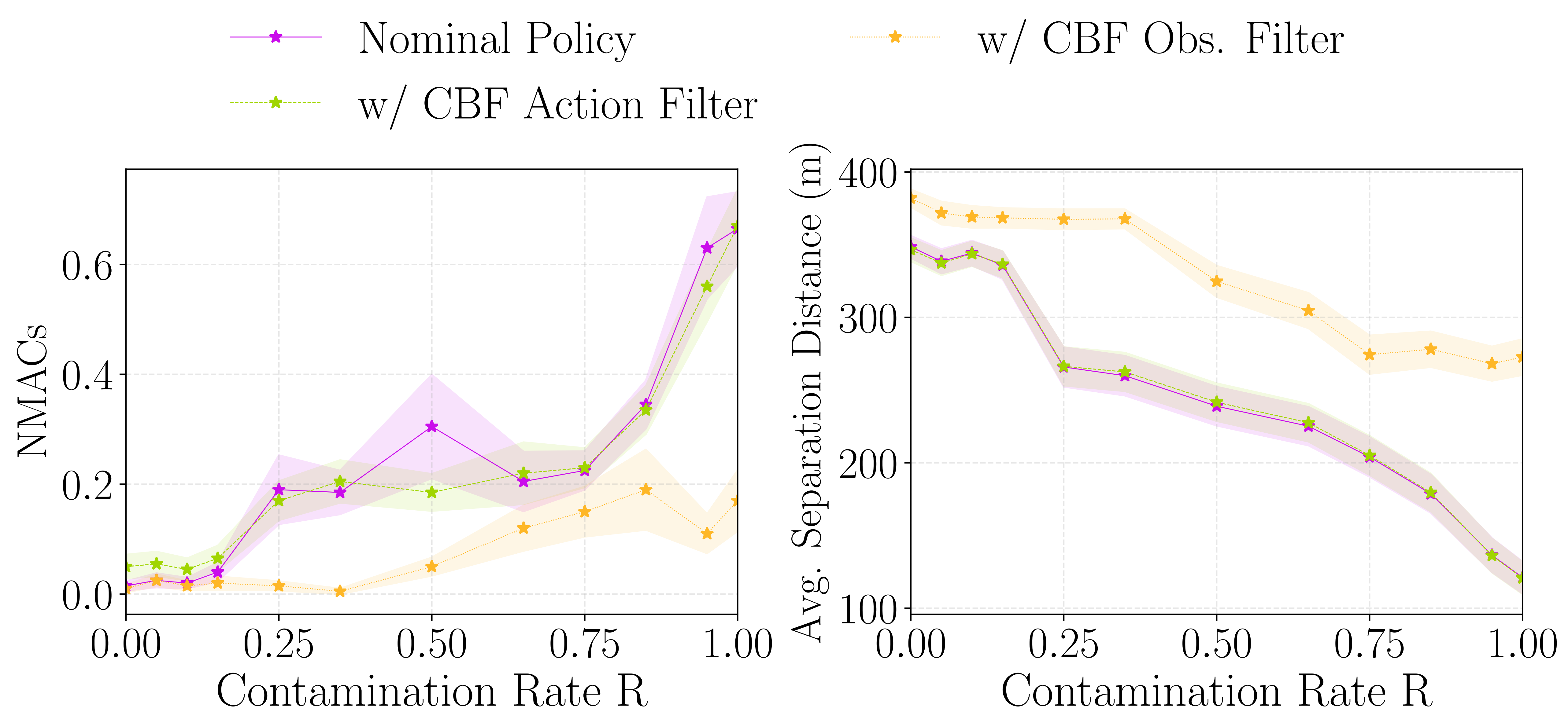
fewer near mid-air collisions

0.24 → 0.02

NMACs per episode

250 m → 375 m

average separation



$R_{max} = 0.7, \quad \alpha = 5\ s$

Observation filtering removes nine near collisions in ten

90%

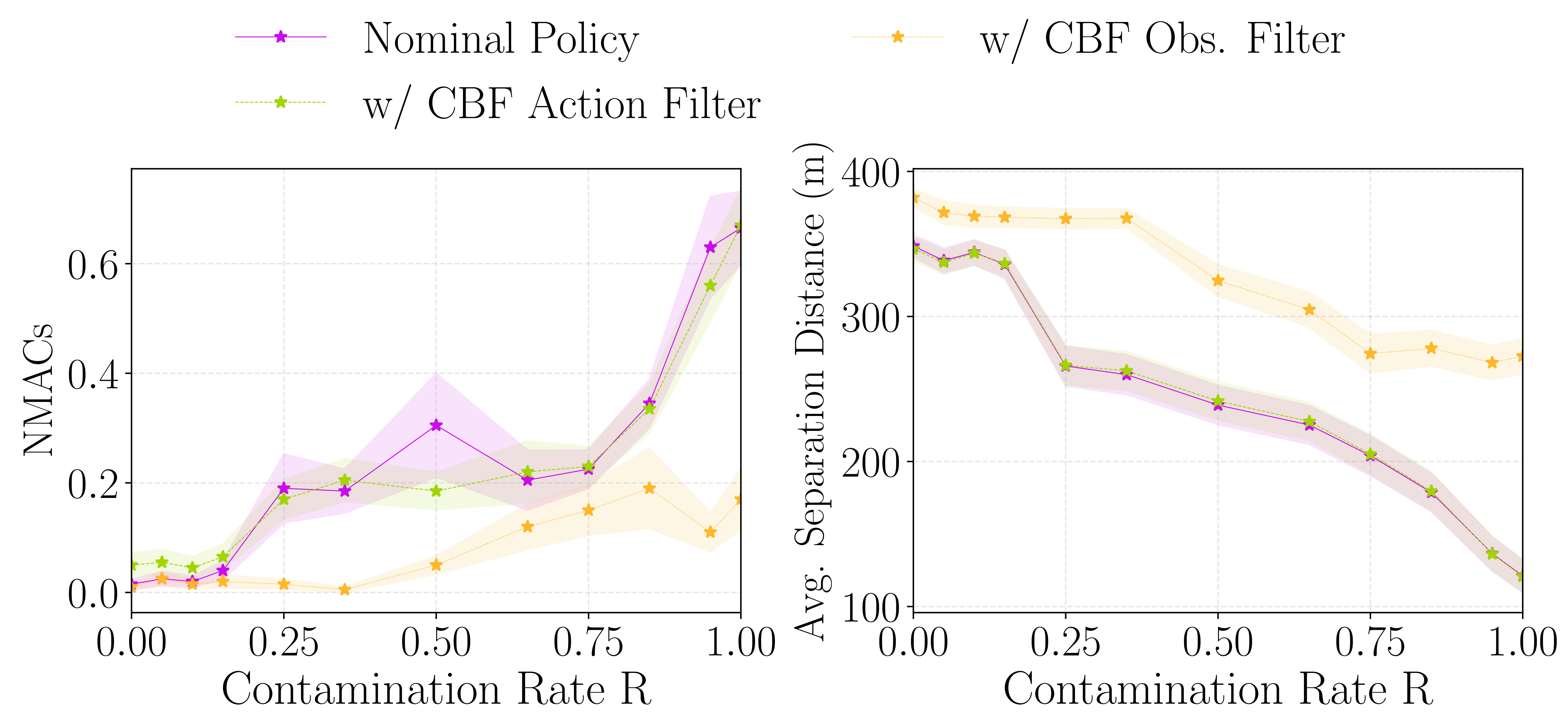
fewer near mid-air collisions

0.24 → 0.02

NMACs per episode

250 m → 375 m

average separation



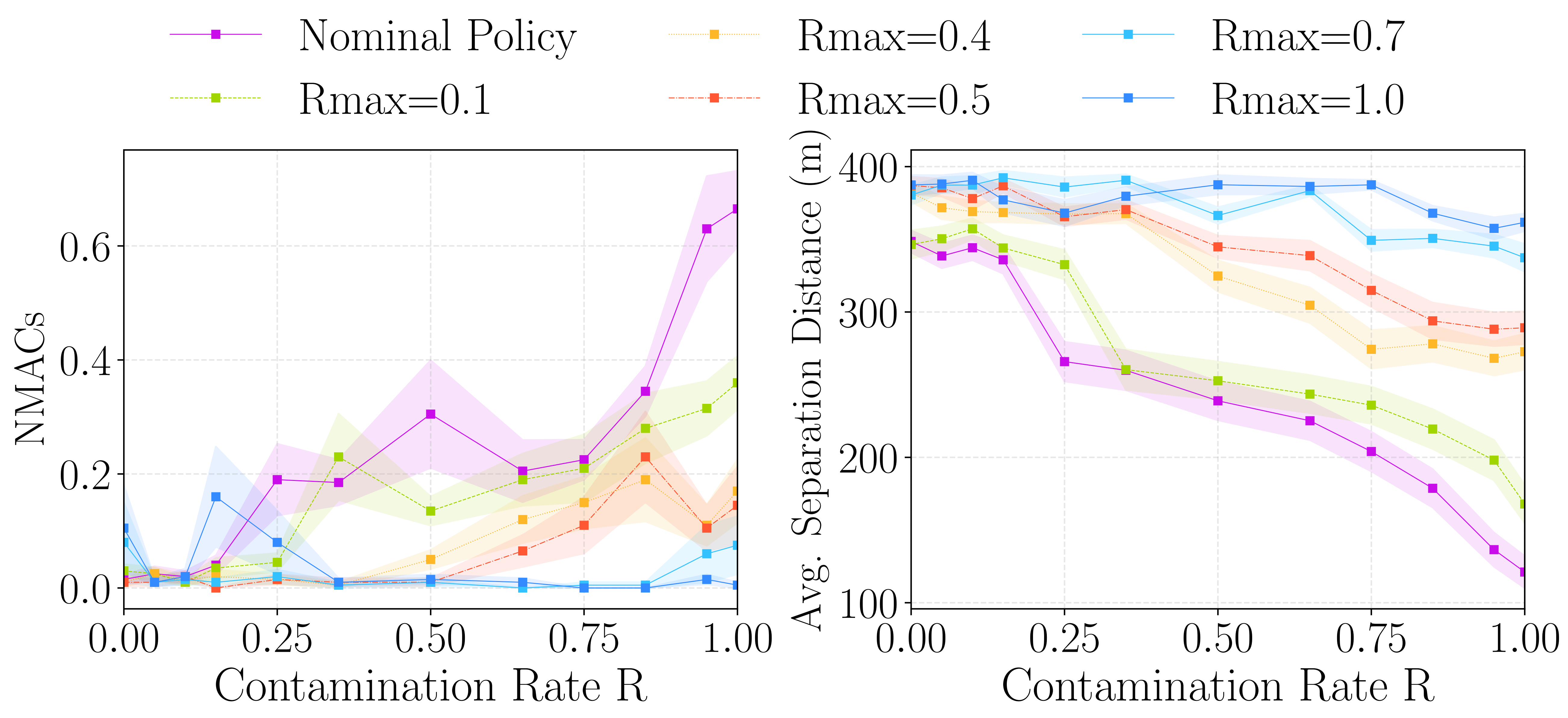
$R_{max} = 0.7, \quad \alpha = 5\ s$

With the same worst-case estimate, the observation filter performs better on its own.

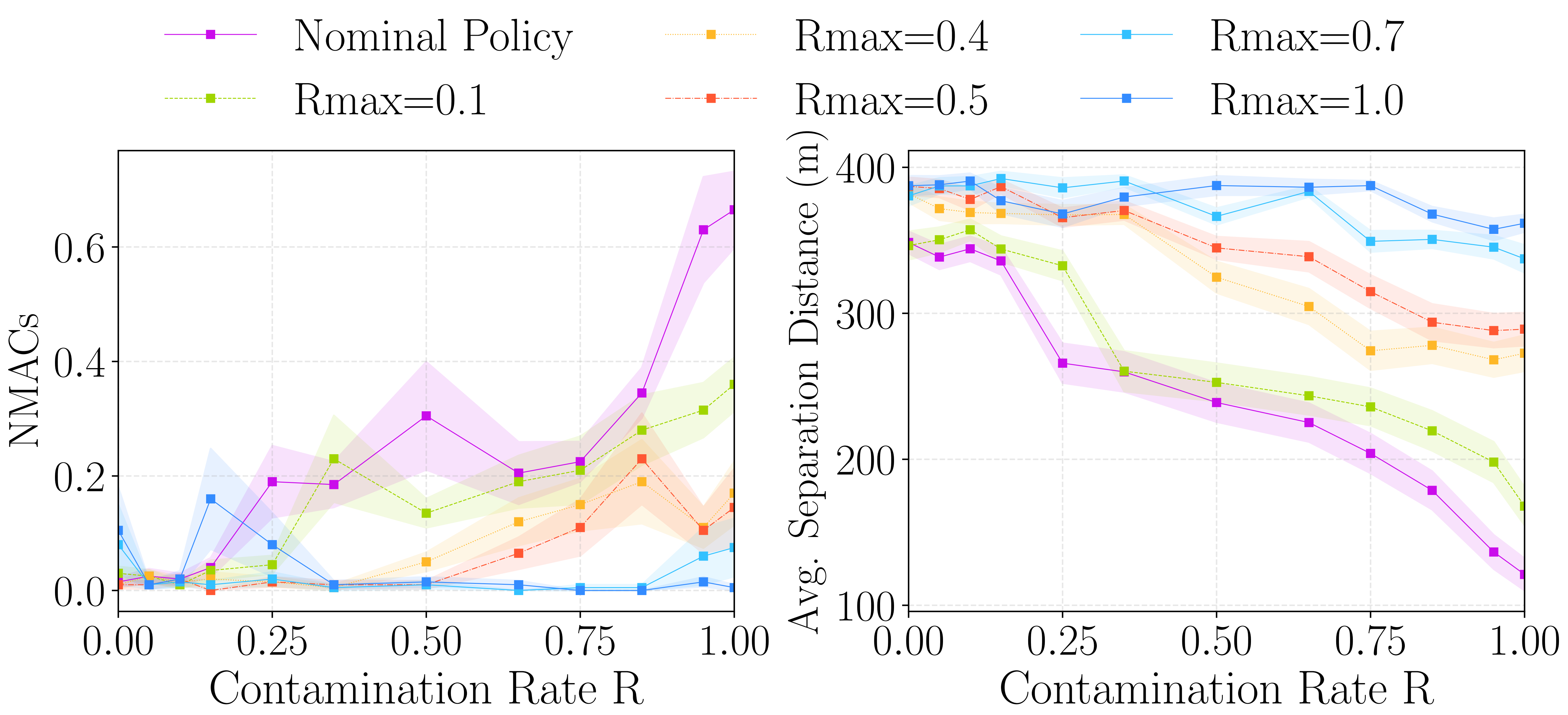
The advantage grows with what the filter assumes

04 RESULTS

The advantage grows with what the filter assumes



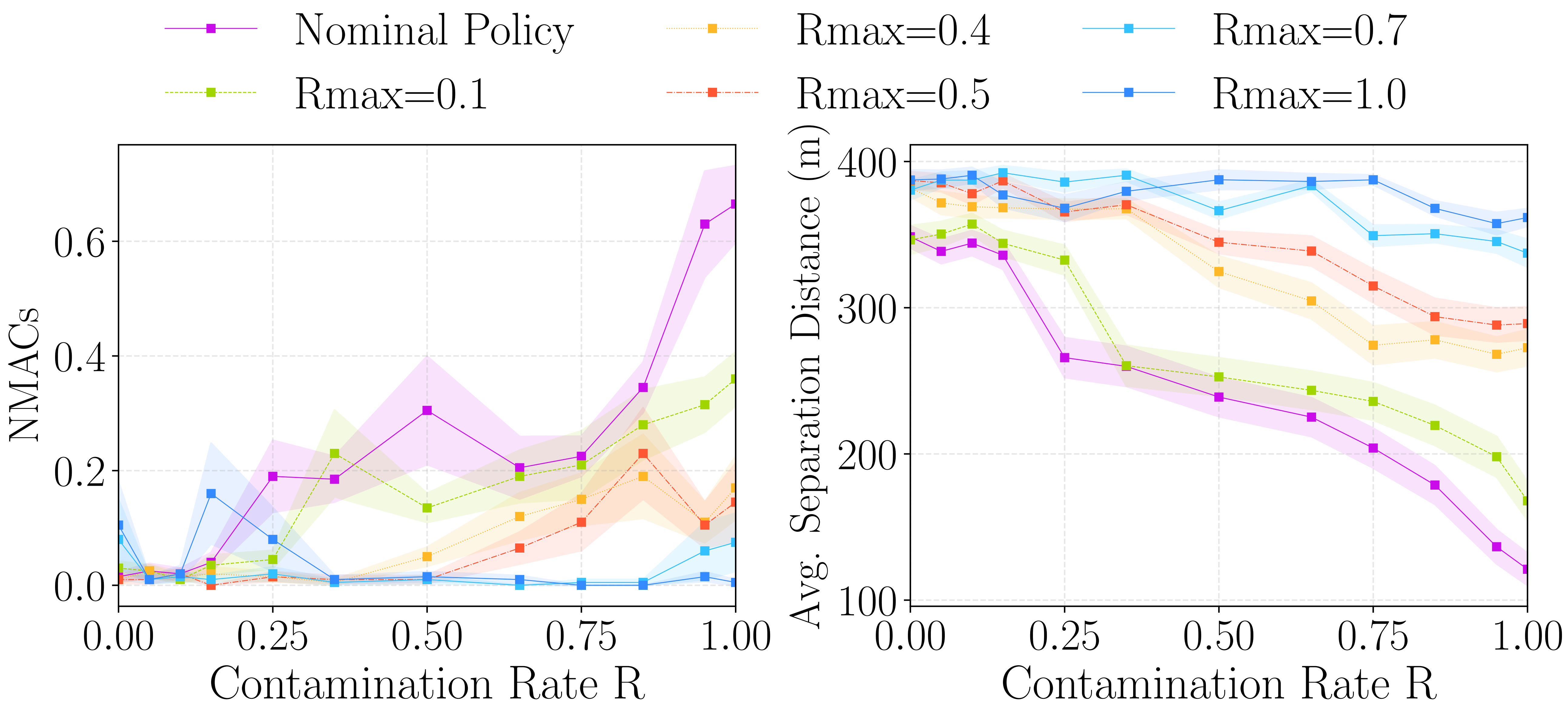
The advantage grows with what the filter assumes



The advantage grows with what the filter assumes

$R_{max} = 0.1 - 0.5$

Little benefit. The assumed bound is too small to surface the danger.



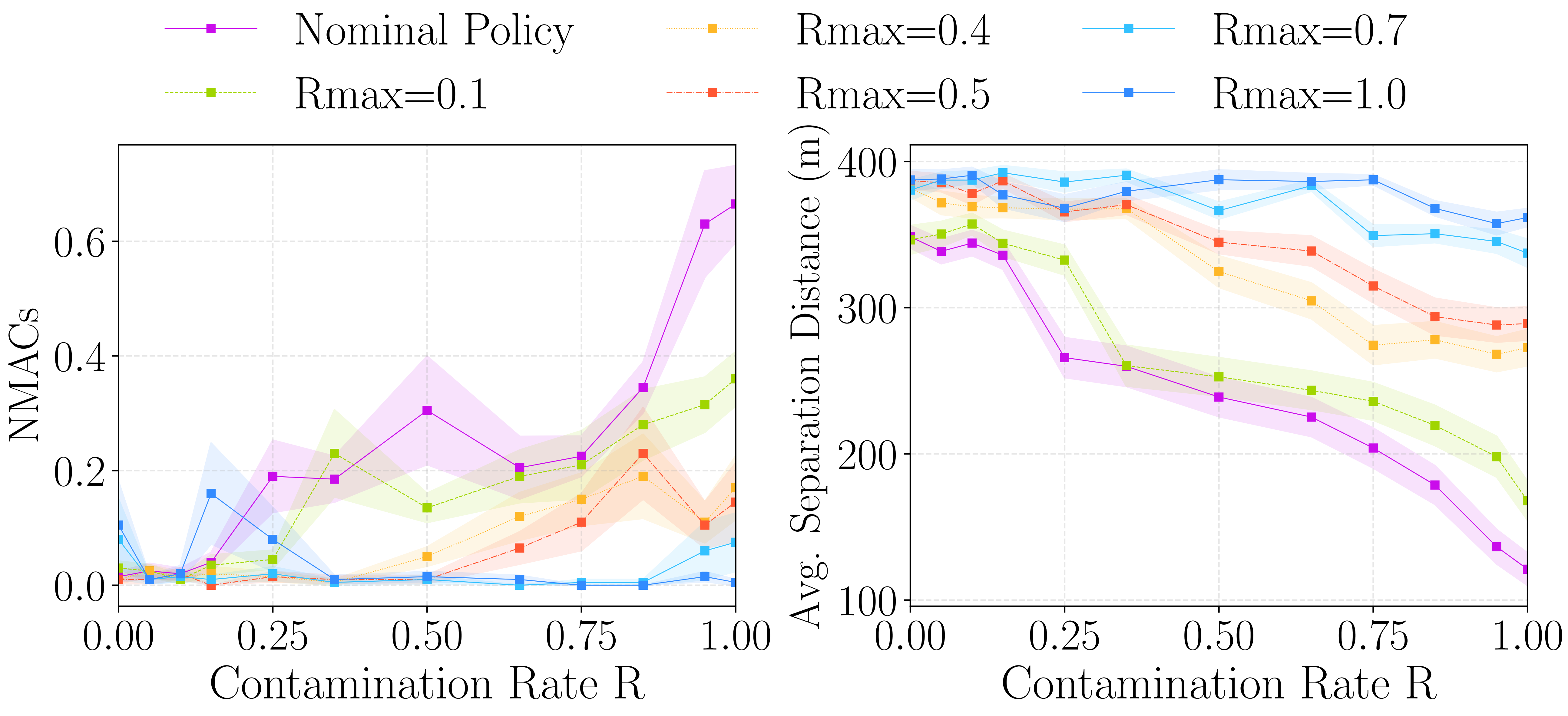
The advantage grows with what the filter assumes

$R_{max} = 0.1 – 0.5$

Little benefit. The assumed bound is too small to surface the danger.

$R_{max} = 0.7 – 1.0$

NMACs are near zero; separation holds around 380 m as nominal policy collapses to 130 m.



The advantage grows with what the filter assumes

$R_{max} = 0.1 - 0.5$

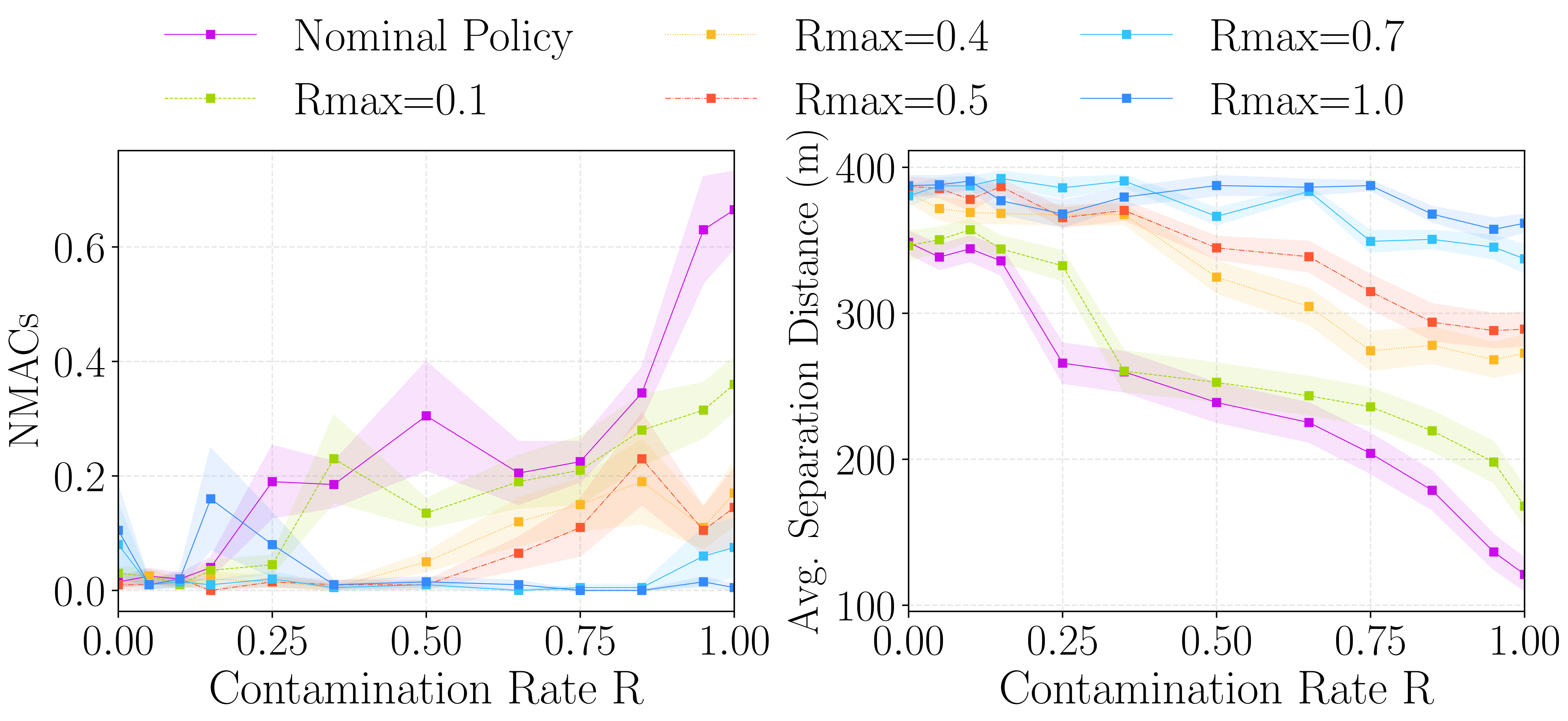
Little benefit. The assumed bound is too small to surface the danger.

$R_{max} = 0.7 - 1.0$

NMACs are near zero; separation holds around 380 m as nominal policy collapses to 130 m.

No tuning

The filter never observes the true R; R_{max} is fixed before deployment.



The advantage grows with what the filter assumes

$R_{max} = 0.1 - 0.5$

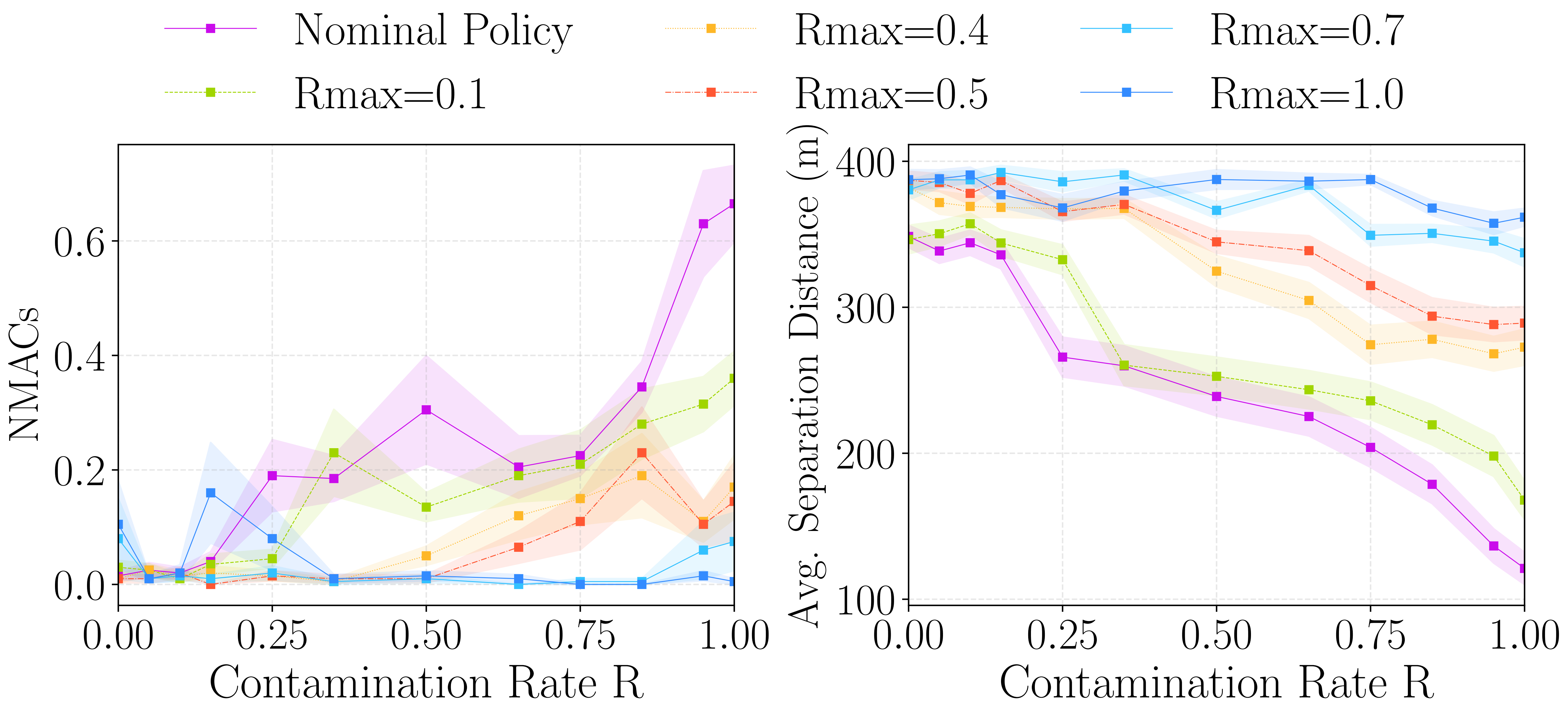
Little benefit. The assumed bound is too small to surface the danger.

$R_{max} = 0.7 - 1.0$

NMACs are near zero; separation holds around 380 m as nominal policy collapses to 130 m.

No tuning

The filter never observes the true R; R_{max} is fixed before deployment.

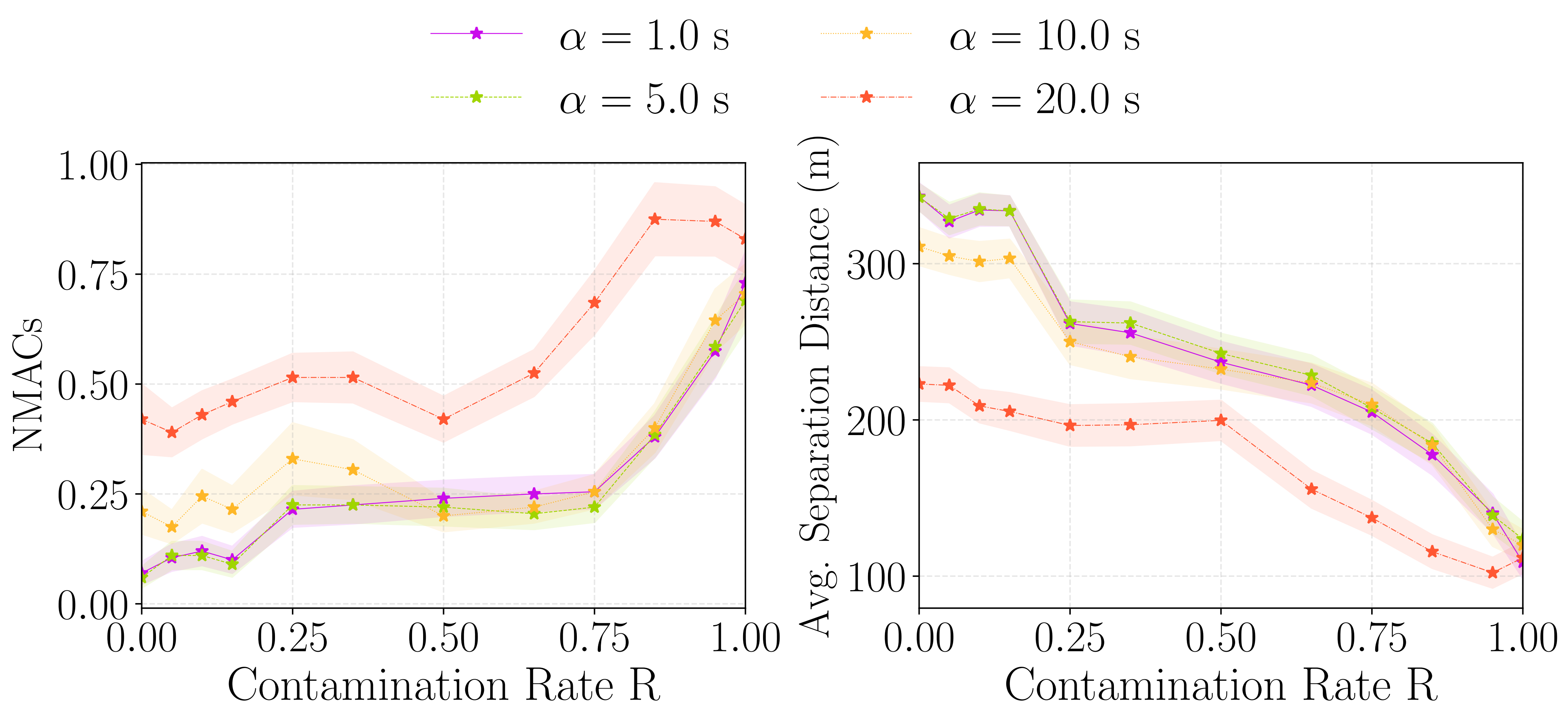


The filter is never told how bad the degradation really is.

Action filtering breaks as α grows; observation filtering does not

Action filtering breaks as α grows; observation filtering does not

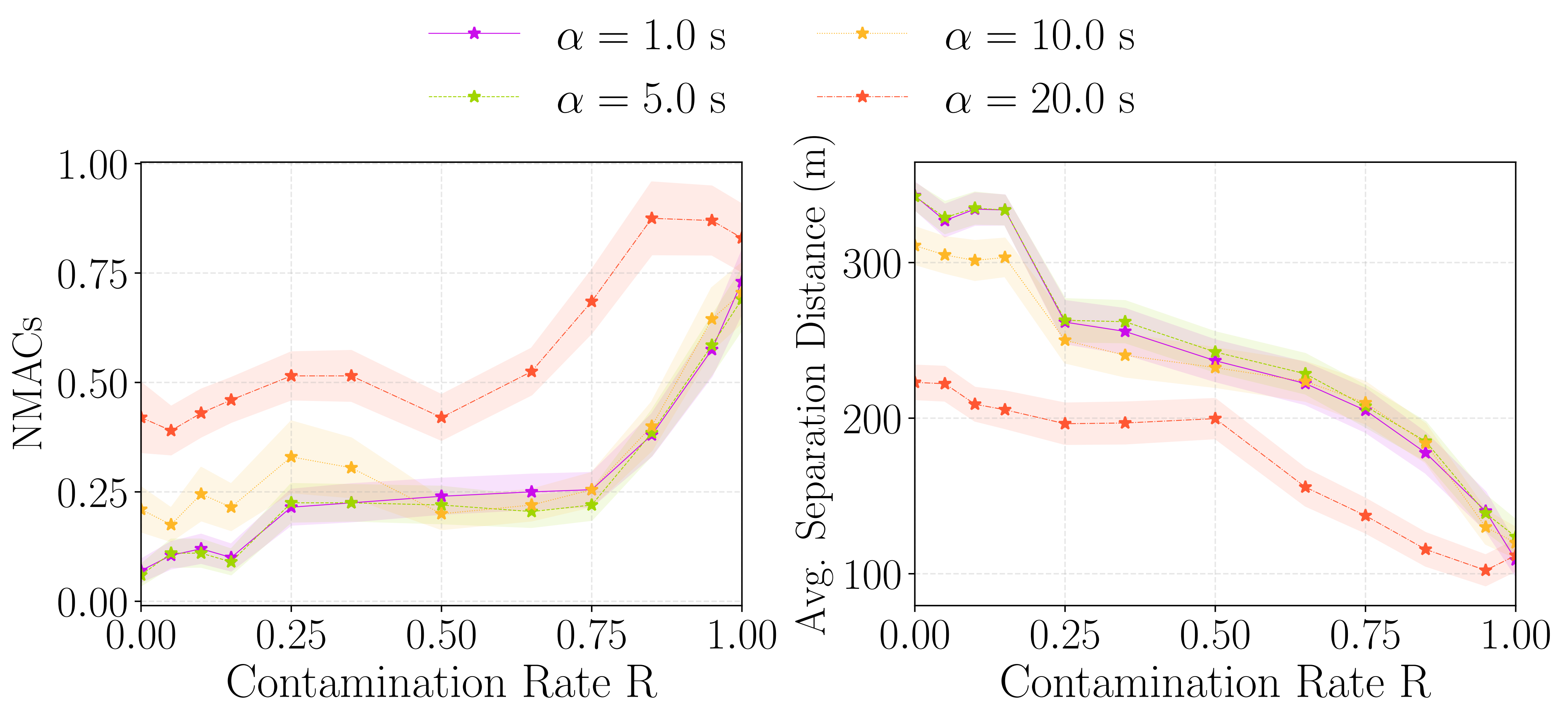
ACTION FILTER



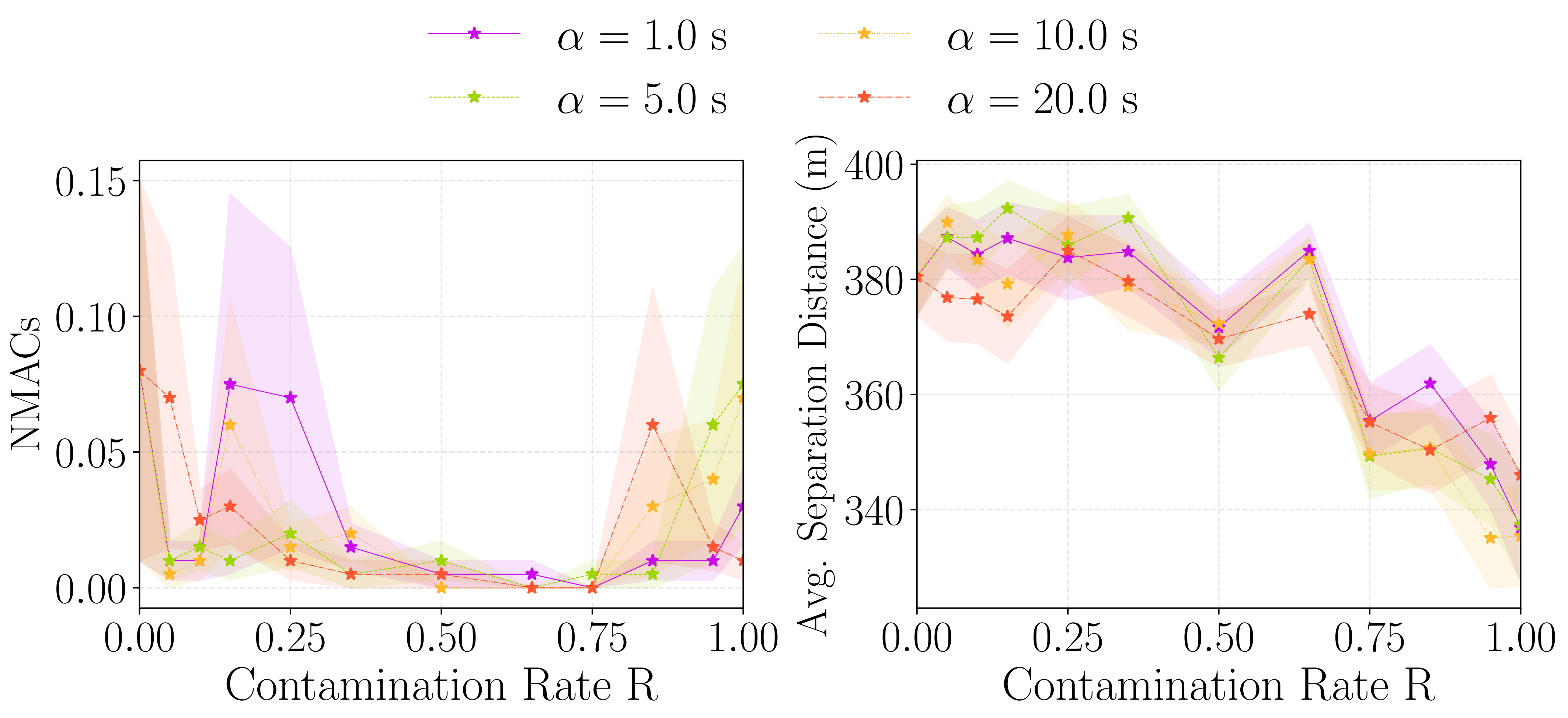
$\alpha = 20\ s$ more than doubles the NMACs.

Action filtering breaks as α grows; observation filtering does not

ACTION FILTER



OBSERVATION FILTER

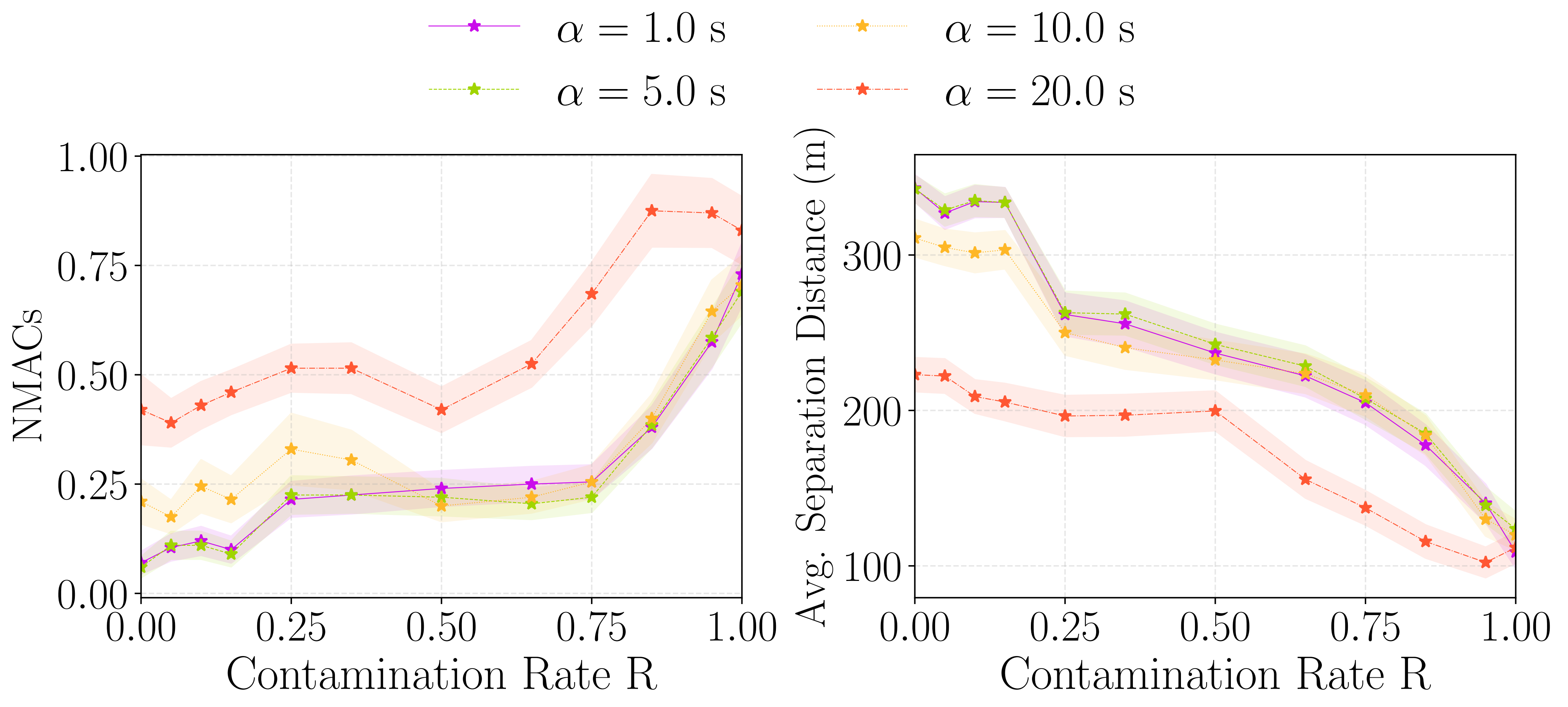


$\alpha = 20\ s$ more than doubles the NMACs.

All α values' effects seem to coincide.

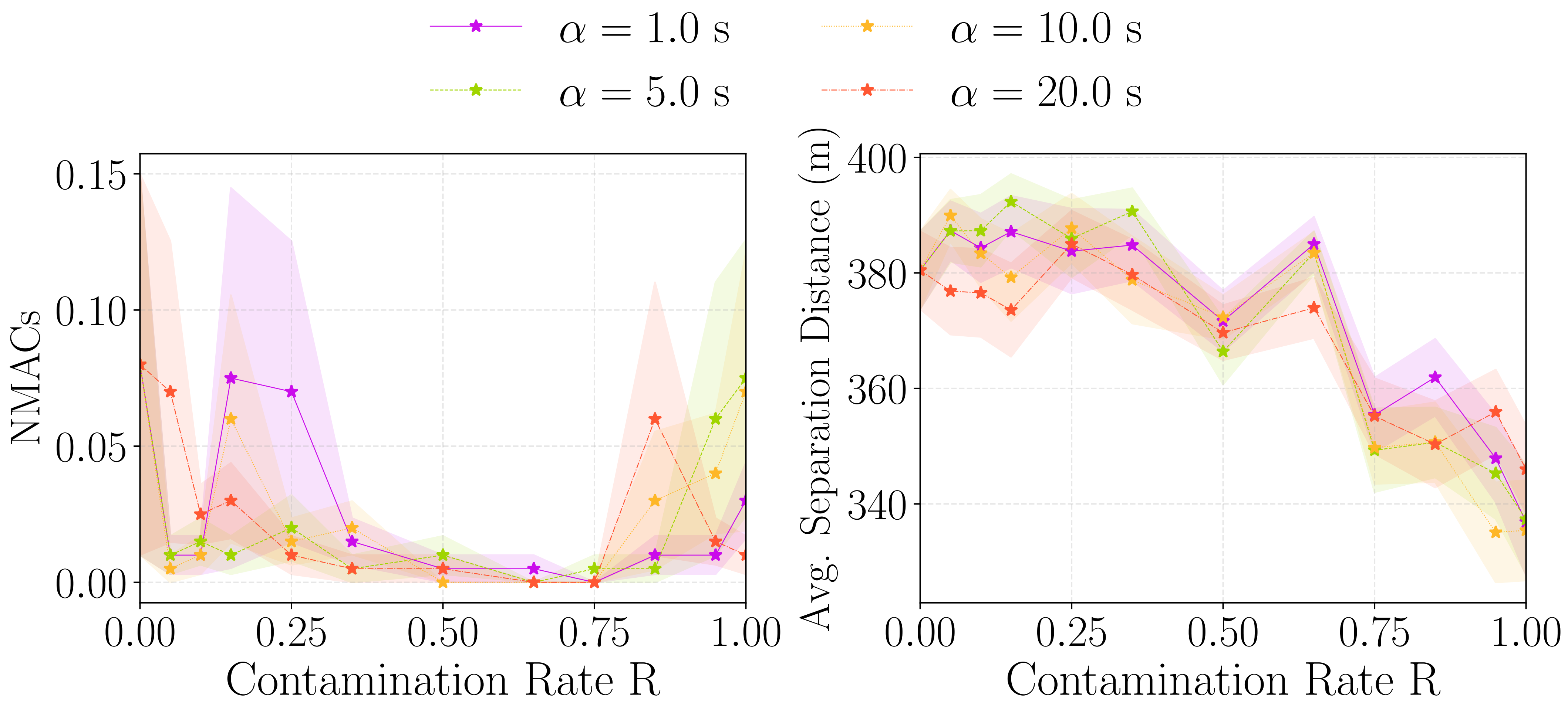
Action filtering breaks as α grows; observation filtering does not

ACTION FILTER



$\alpha = 20\ s$ more than doubles the NMACs.

OBSERVATION FILTER

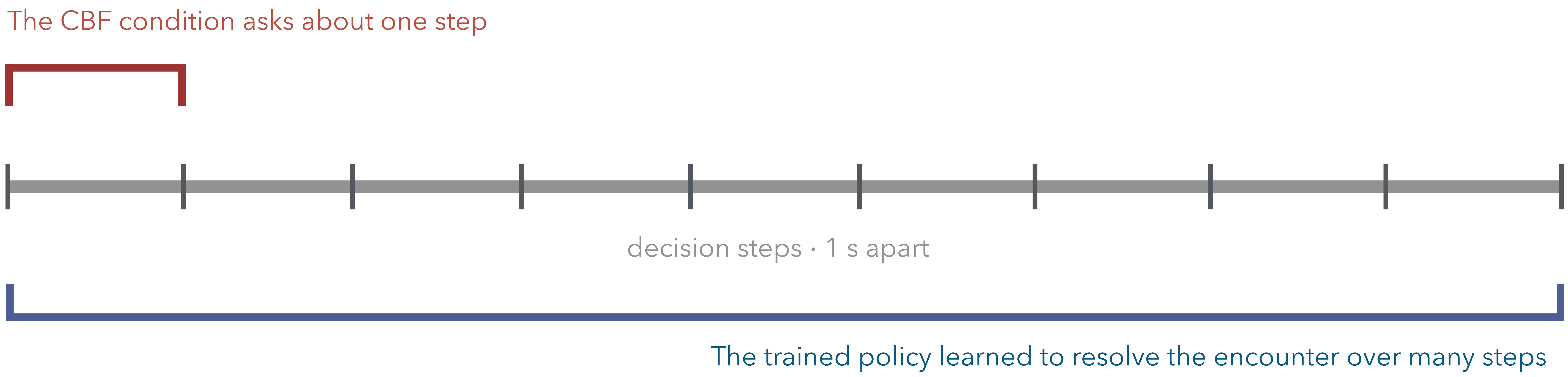


All α values' effects seem to coincide.

α is a barrier-function parameter. It matters only where the barrier can veto the policy's action.

05 WHY

The barrier looks one step ahead; the policy looks further



Action filtering replaces multi-step reasoning with a single-step test.

Preserve the trained policy's decision authority

When a learned controller has internalized safety behavior,
informing it outweighs overriding its decision.

Preserve the trained policy's decision authority

When a learned controller has internalized safety behavior,
informing it outweighs overriding its decision.

ACTION FILTERING

No measurable safety gain; highly sensitive to the filtering assumptions.

06 TAKEAWAYS

Preserve the trained policy's decision authority

When a learned controller has internalized safety behavior,
informing it outweighs overriding its decision.

ACTION FILTERING

No measurable safety gain; highly sensitive to the filtering assumptions.

OBSERVATION FILTERING

Could be more effective depending on how the policy was trained.

Preserve the trained policy’s decision authority

When a learned controller has internalized safety behavior,
informing it outweighs overriding its decision.

ACTION FILTERING

No measurable safety gain; highly sensitive to the filtering assumptions.

OBSERVATION FILTERING

Could be more effective depending on how the policy was trained.

THE COST

Conservatism, e.g., earlier and more frequent slowing down.

Digital Avionics Systems Conference
Orlando, Florida, USA - September 13-17, 2026

Thank you!

Questions?

Runtime Safety Filtering for Learned Small UAS Separation Policies under GNSS Degradation

Alex Zongo · Peng Wei
Department of Mechanical and Aerospace Engineering
George Washington University, Washington, DC, USA.

Contact: a.zongo@gwu.edu

Preprint: arXiv:2607.10014