Software Rejuvenation for Safe Operation of Cyber-Physical Systems in the Presence of Run-time Cyber Attacks

Carnegie Mellon University
Software Engineering Institute

AUGUST 16, 2023

Raffaele Romagnoli, Bruce Krogh, **Dionisio de Niz**, Anton Hristozov, Bruno Sinopoli

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Copyright 2023 Carnegie Mellon University, Bruce Krogh and Bruno Sinopoli.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

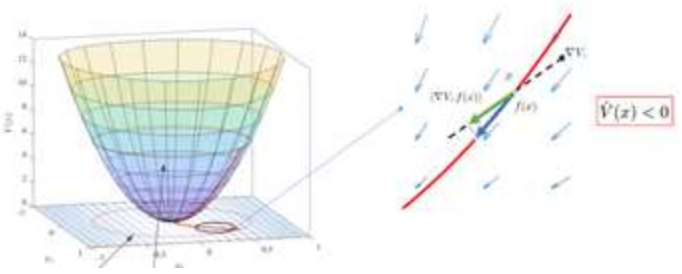
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

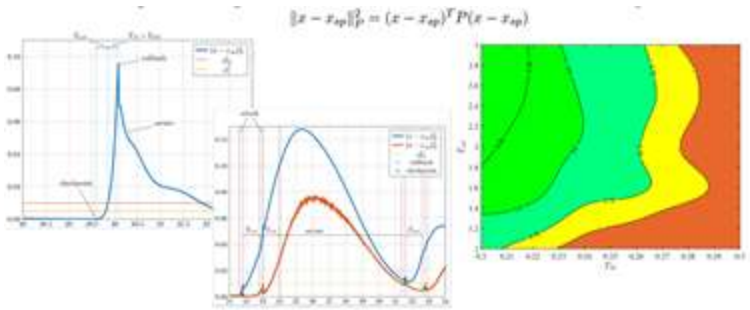
DM23-0803

Outline

1. **Introduction to Software Rejuvenation**
   a. Flight Control Software Architecture
   b. Cyber Attack Exposure
   c. Software Refresh\Rollback
   d. Periodic vs Aperiodic SR
2. **Proposed Software Rejuvenation Solution**
   a. Ensuring Safety and Safe Tracking
   b. Software Rejuvenation Scheme
3. **Safety and Quadratic Boundedness**
   a. Empirical method for SR design
   b. Results
4. **Conclusions**

crazyflie

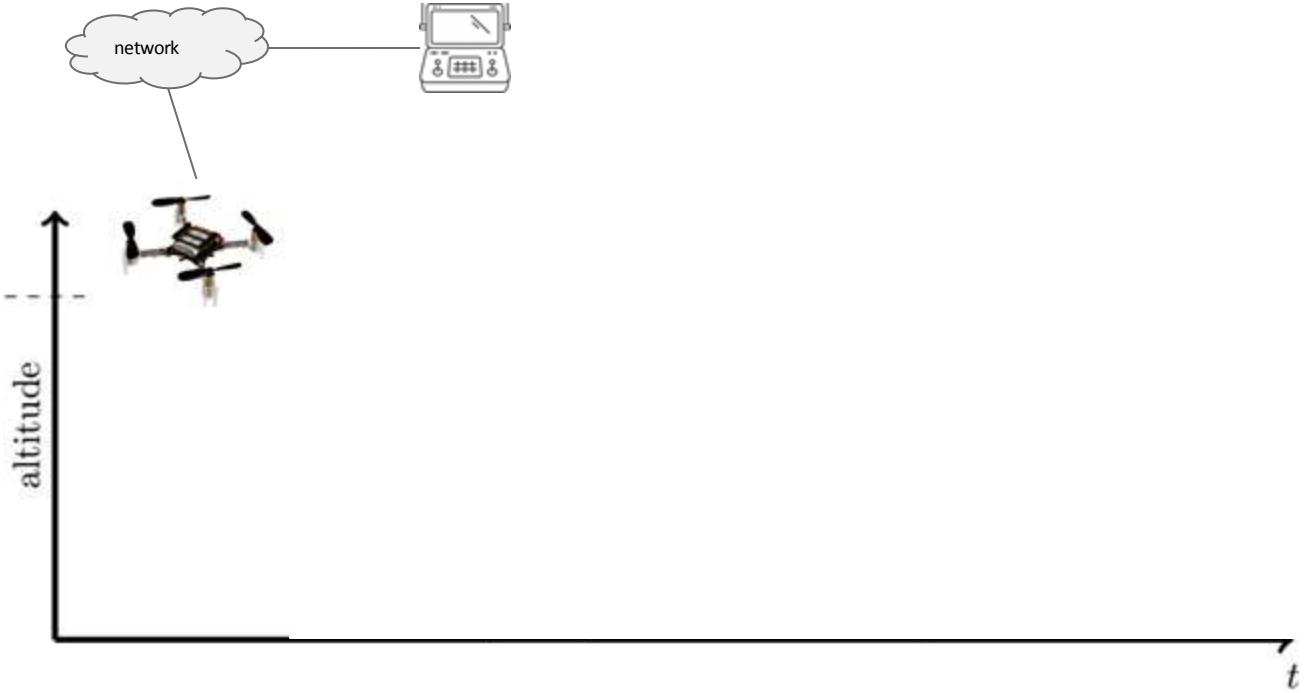




© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

1 - Introduction to Software Rejuvenation



Mission

- Hovering

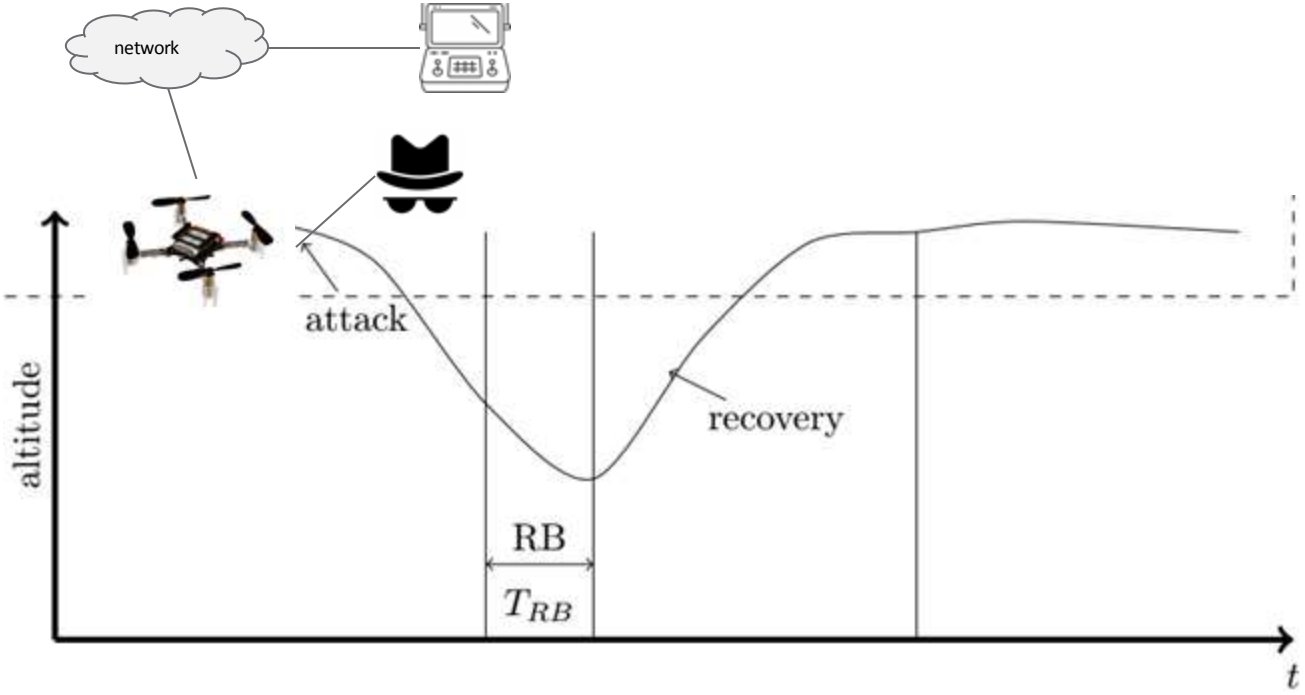
Communication

- Connected to the network

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

1.c - Software Refresh/Rollback



Mission

- Hovering

Communication

- Connected to the network
  - PX4 : Mavlink

Cyber attacks

- On the run-time code

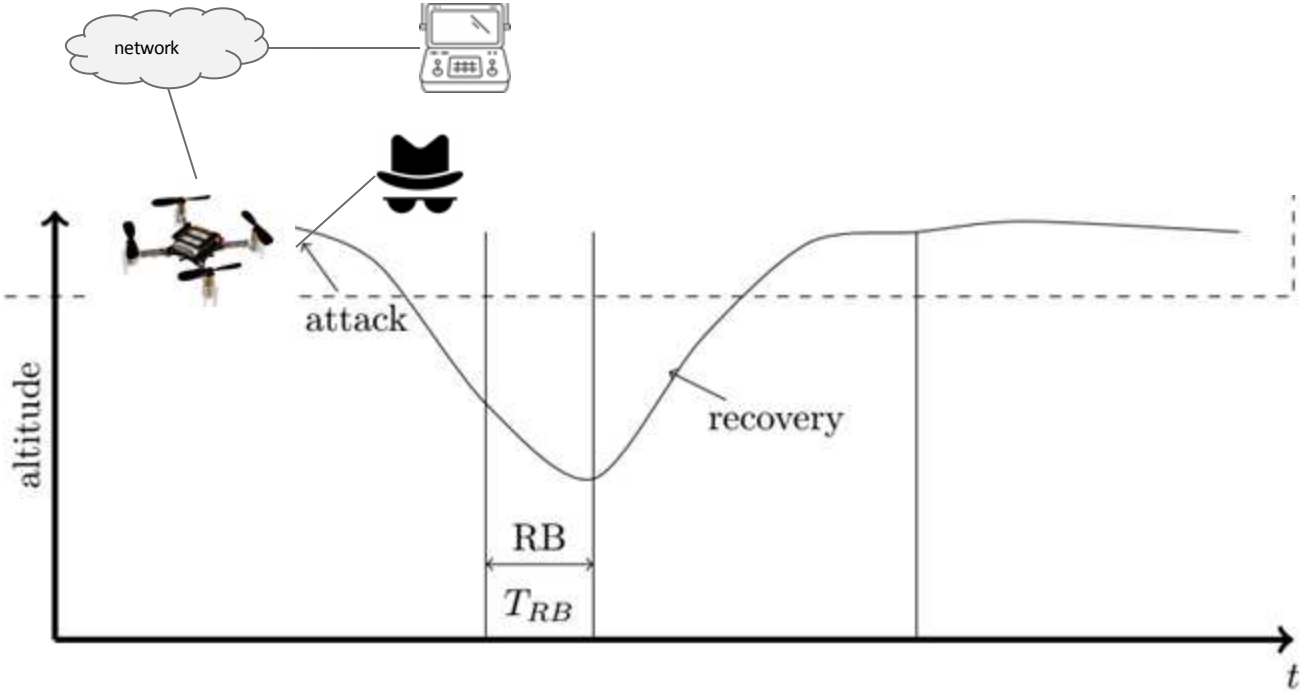
Idea

- **Software Reset/Rollback**

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

1.d - Periodic vs Aperiodic Rollback



Mission
- Hovering

Communication
- Connected to the network
  - PX4 : Mavlink

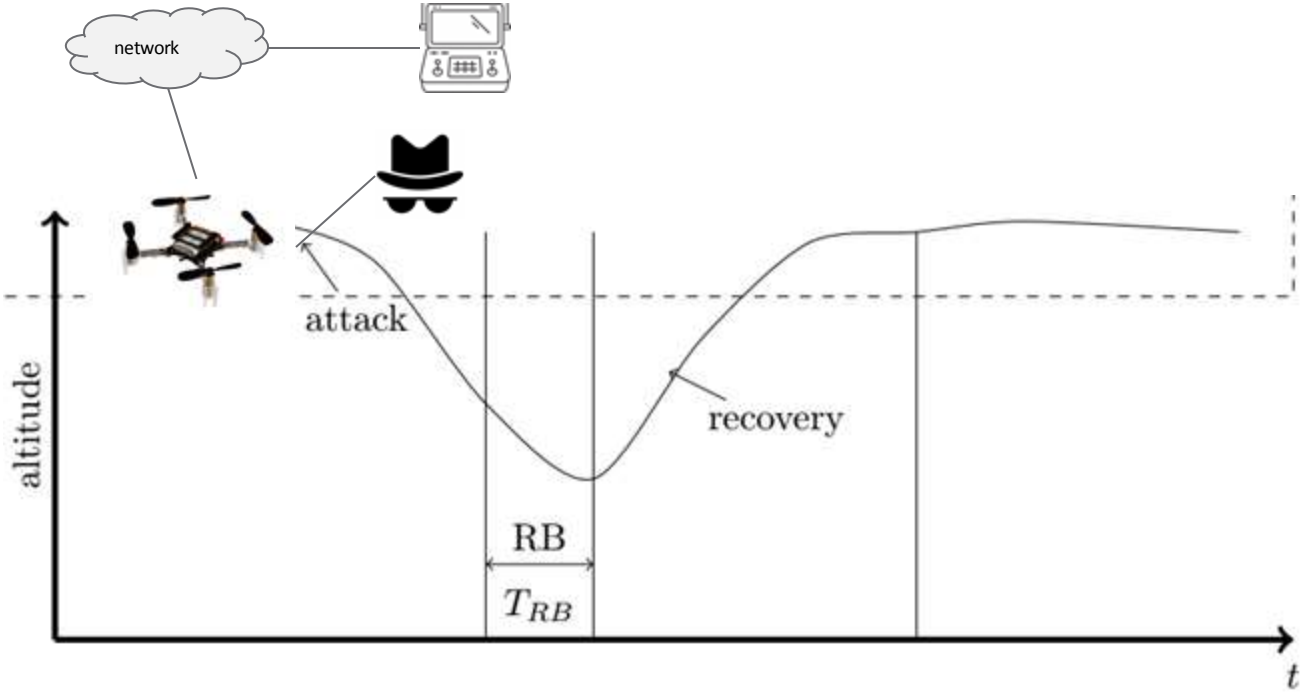
Cyber attacks
- On the run-time code

Idea
- **Software Reset/Rollback**

★ Periodic Reboot - (Focus on the Security) [Arroyo et al 2017]
★ On-line Reach set analysis - (Focus on the Performance) [Abdi et al 2019]

© 2023 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution.

1.d - Periodic vs Aperiodic Rollback



★ Periodic Reboot - (Focus on the Security) [Arroyo et al 2017]

★ On-line Reach set analysis - (Focus on the Performance) [Abdi et al 2019]

Mission

- Hovering

Communication

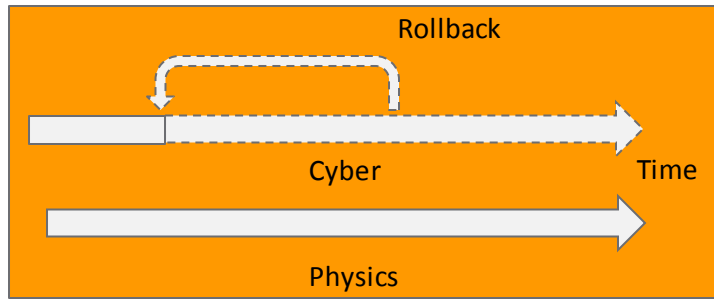
- Connected to the network
  - PX4 : Mavlink

Cyber attacks

- On the run-time code

Idea

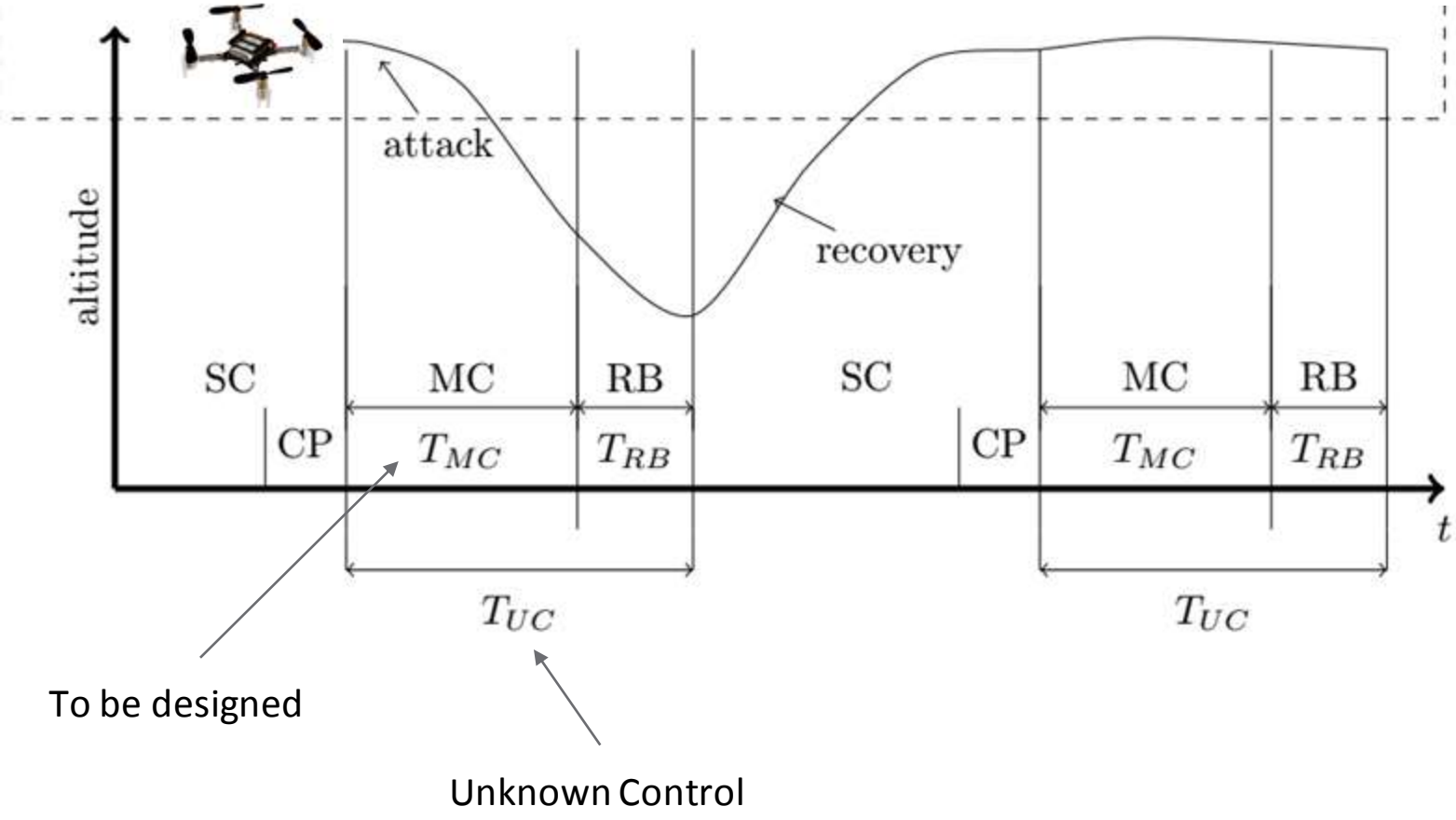
- **Software Reset/Rollback**



© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

2 - Proposed Software Rejuvenation Solution

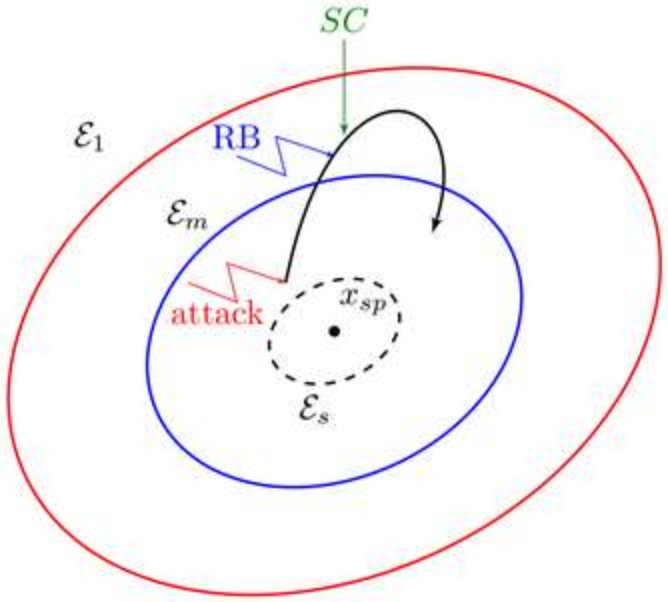


- SC - Secure Control
- CP - Checkpoint
- MC - Mission Control
- RB - Rollback

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

2.a - Ensuring Safety and Safe Tracking



$$\|x - x_{sp}\|_P^2 = (x - x_{sp})^T P (x - x_{sp})$$

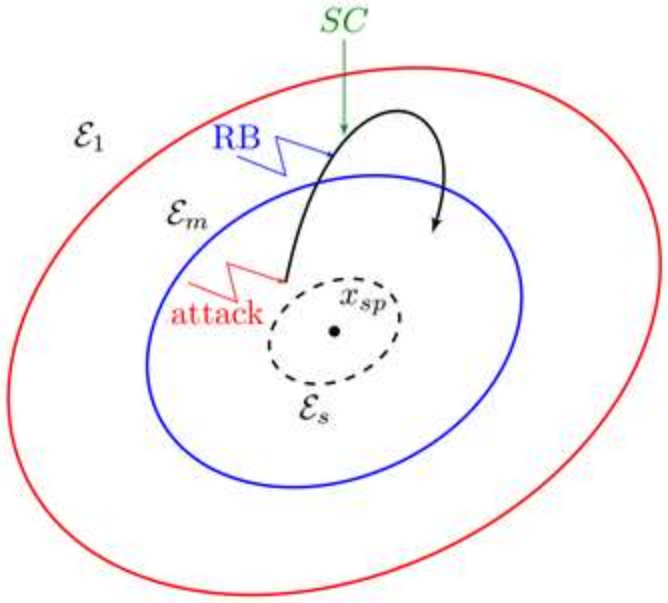
$$\mathcal{E}_c = \left\{ x \in \mathbb{R}^n : \|x - x_{sp}\|_P^2 \leq c \right\}$$

$$s < m < 1 \Rightarrow \mathcal{E}_s \subset \mathcal{E}_m \subset \mathcal{E}_1$$

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

2.a - Ensuring Safety and Safe Tracking



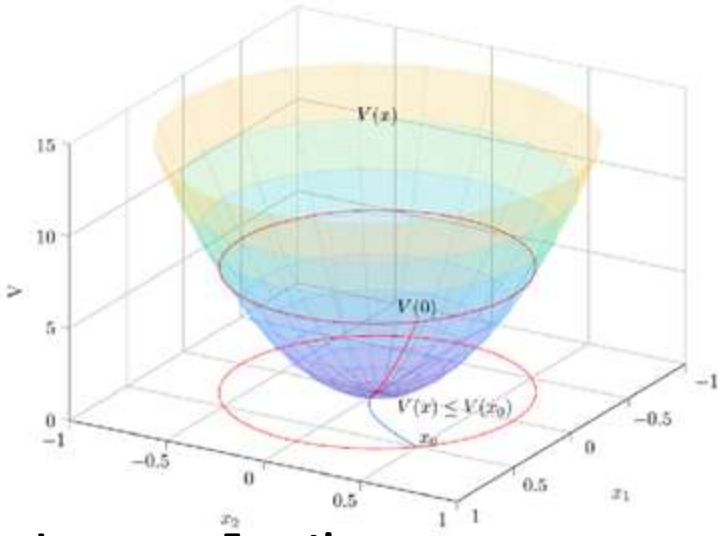
$$\|x - x_{sp}\|_P^2 = (x - x_{sp})^T P (x - x_{sp})$$

$$\mathcal{E}_c = \left\{ x \in \mathbb{R}^n : \|x - x_{sp}\|_P^2 \leq c \right\}$$

$$s < m < 1 \Rightarrow \mathcal{E}_s \subset \mathcal{E}_m \subset \mathcal{E}_1$$

Lyapunov Theory

$$\dot{x} = f(x) = Ax$$



Lyapunov Function

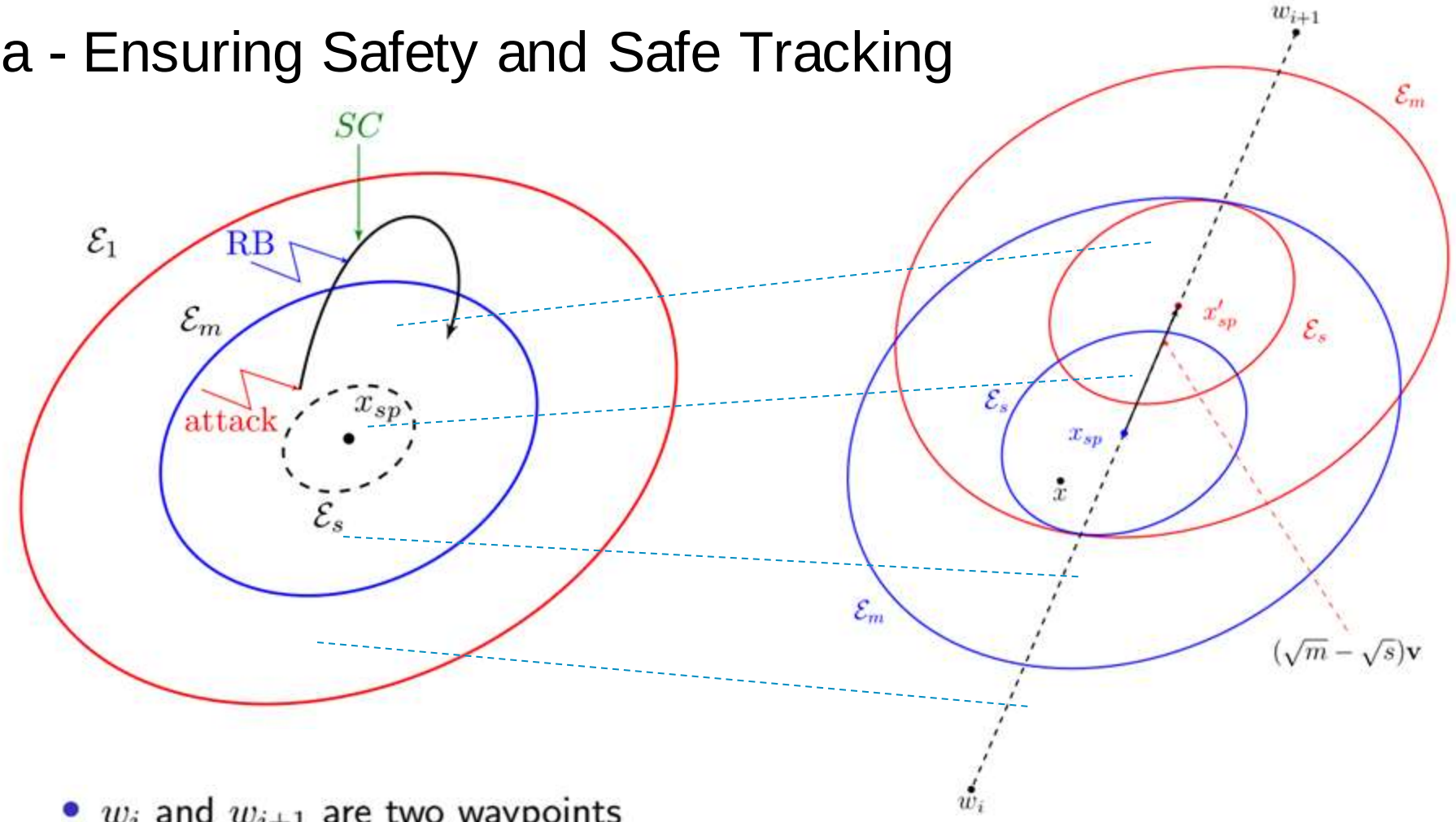
$$V(x) = \|x - x_{sp}\|_P^2 \qquad \dot{V}(x) < 0$$

- $\mathcal{E}_c$ is **positively invariant**

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

2.a - Ensuring Safety and Safe Tracking

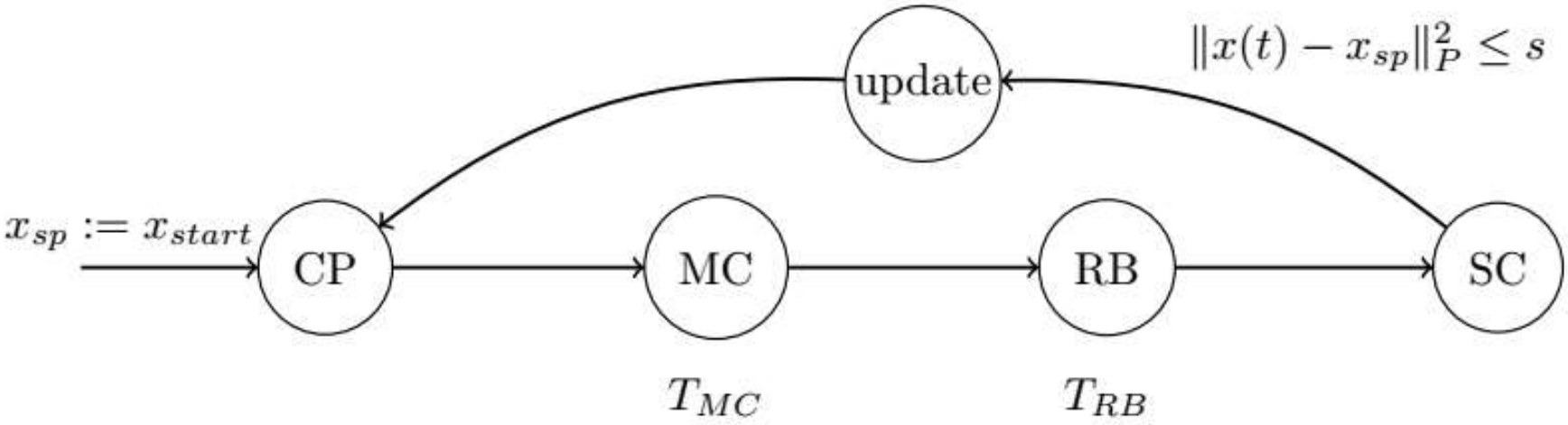


- w_i and w_{i+1} are two waypoints

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

2.b - Software Rejuvenation Scheme

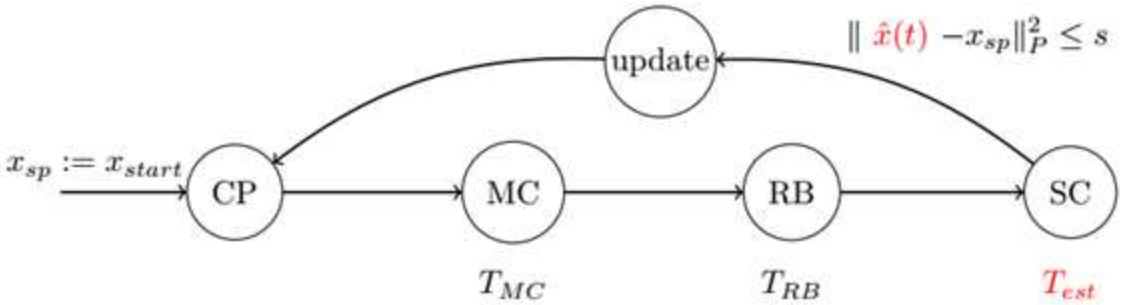


$$x(t) \longrightarrow \hat{x}(t)$$

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

3 - Safety and Quadratic Boundedness

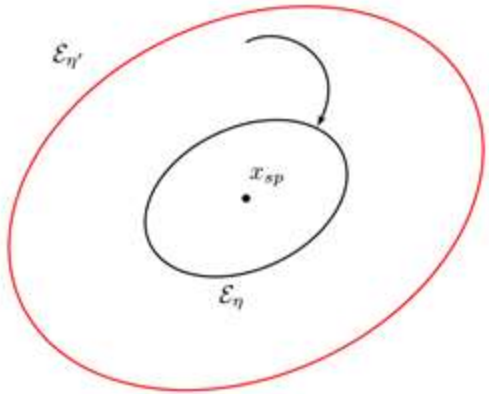


Quadratic Boundedness

$$\dot{x} = Ax + Dd, \quad \|d\| \leq \delta$$

$$V(x) = \|x - x_{sp}\|_P^2$$

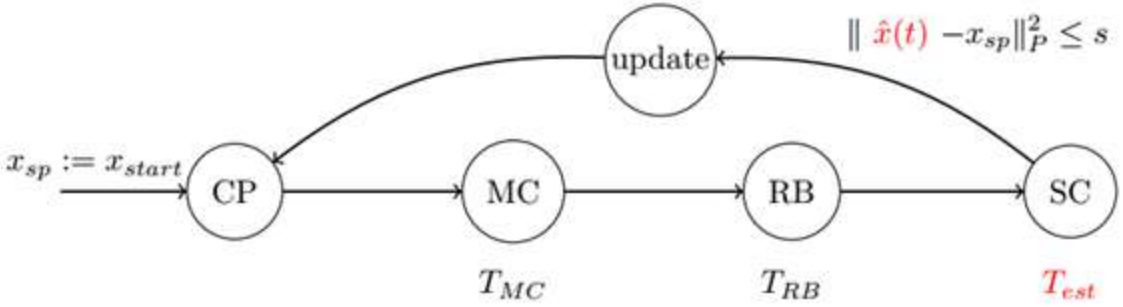
$$V(x) > \eta \rightarrow \dot{V}(x) < 0$$



© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

3 - Safety and Quadratic Boundedness



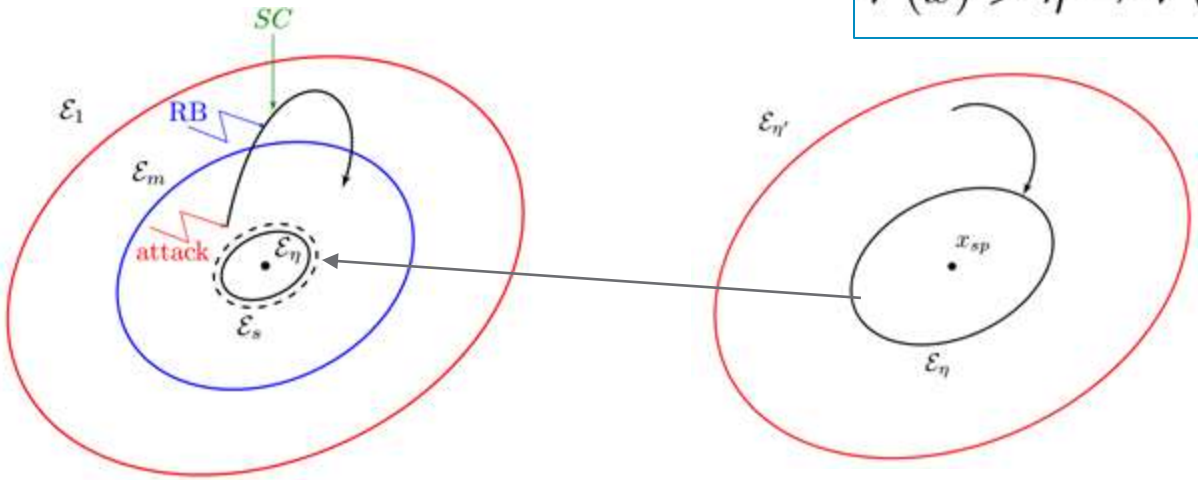
Quadratic Boundedness

$$\dot{x} = Ax + Dd, \quad \|d\| \leq \delta$$

$$V(x) = \|x - x_{sp}\|_P^2$$

$$V(x) > \eta \rightarrow \dot{V}(x) < 0$$

- Estimation error due to SR.
- Model approximations

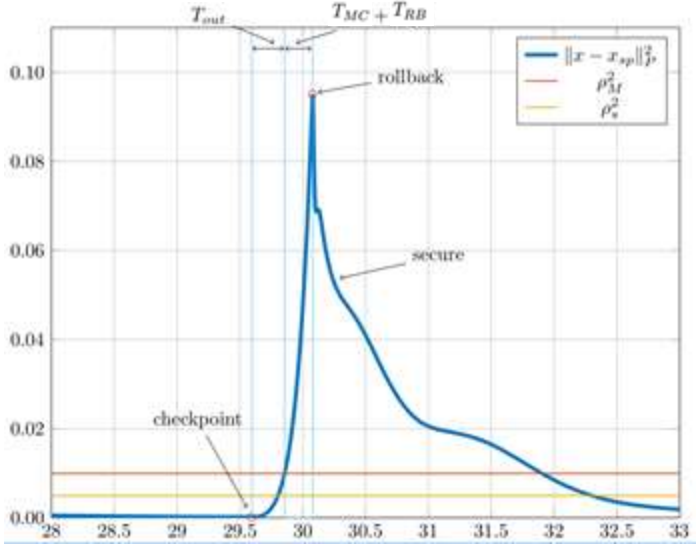


0

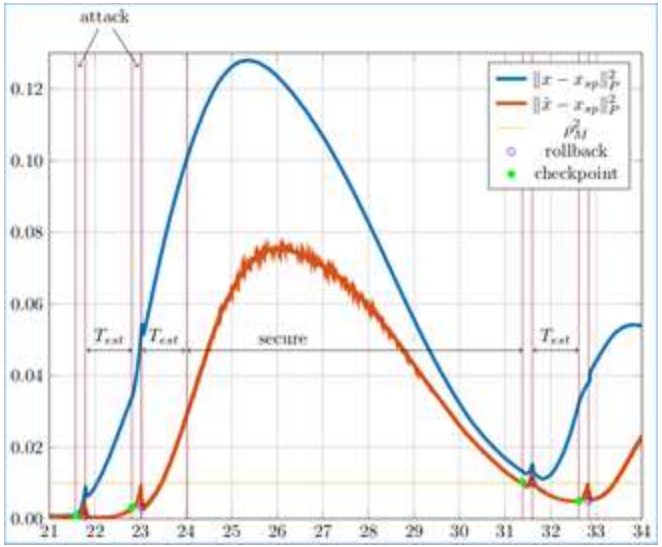
© 2023 Carnegie Mellon University

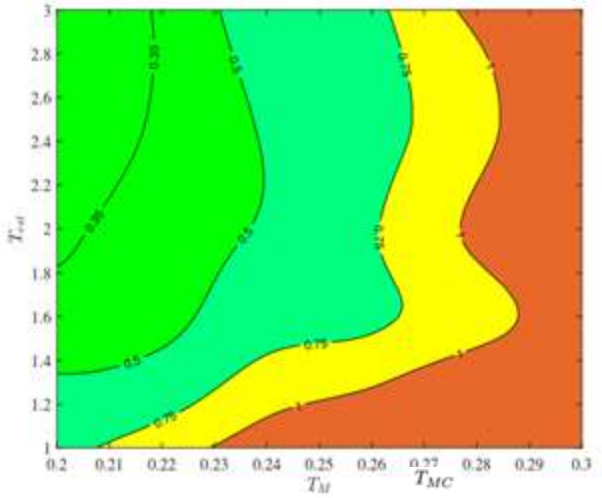
[Distribution Statement A] Approved for public release and unlimited distribution.

3.a - Empirical Method for SR Design



$$\|x - x_{sp}\|_P^2 = (x - x_{sp})^T P (x - x_{sp})$$



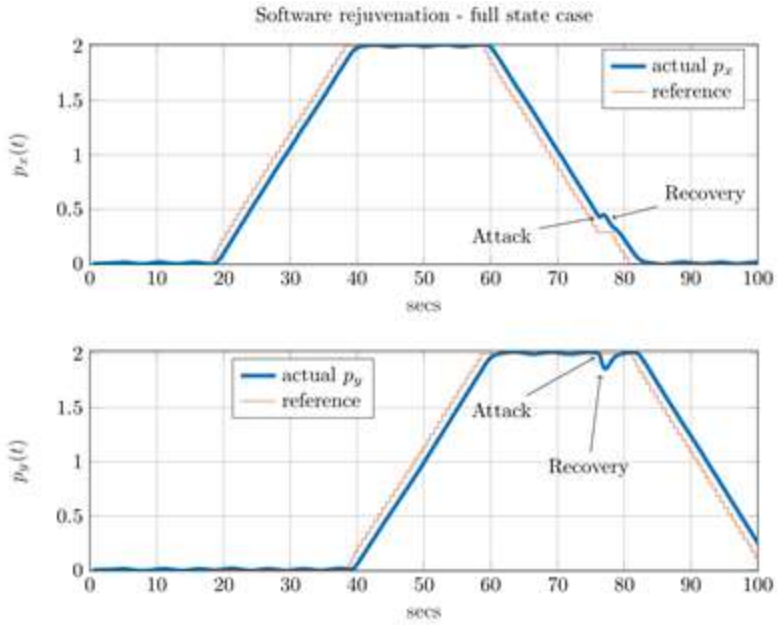


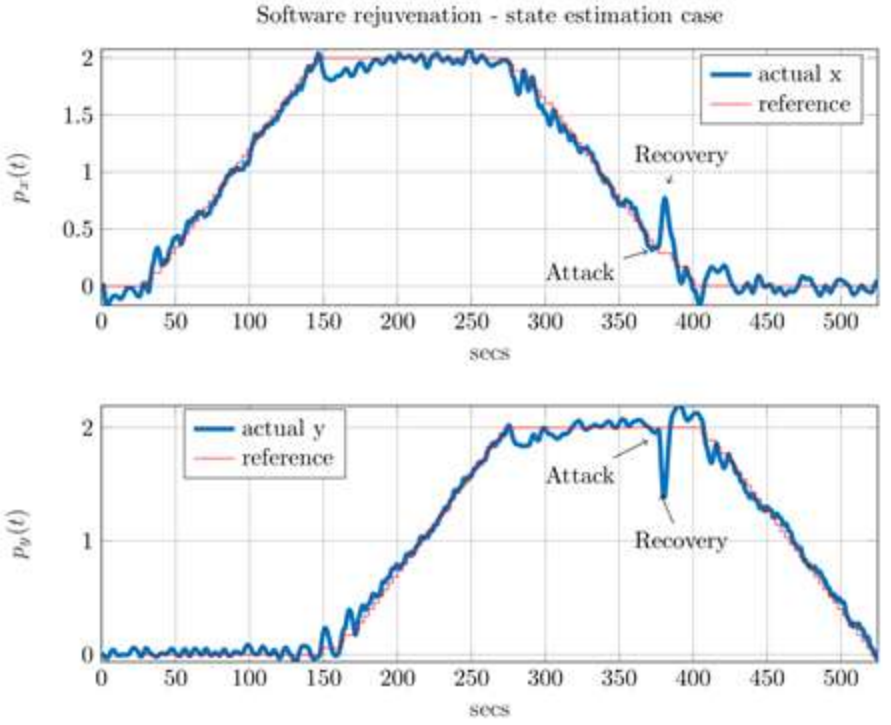
R. Romagnoli, B.H. Krogh, D. de Niz, A. Hristozov, B. Sinopoli. "Software Rejuvenation for Safe Operation of Cyber-Physical Systems in the Presence of Run-time Cyber Attacks". IEEE Transactions on Control System Technology. 2023.

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

3.b - Results



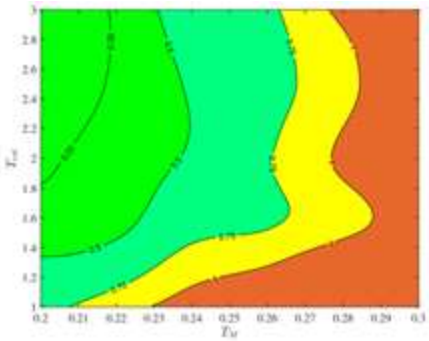


R. Romagnoli, B.H. Krogh, D. de Niz, A. Hristozov, B. Sinopoli. "Software Rejuvenation for Safe Operation of Cyber-Physical Systems in the Presence of Run-time Cyber Attacks". IEEE Transactions on Control System Technology. 2023.

© 2023 Carnegie Mellon University

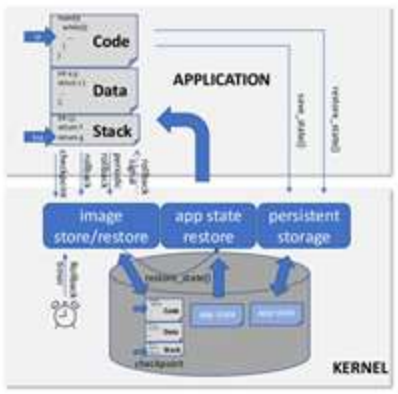
[Distribution Statement A] Approved for public release and unlimited distribution.

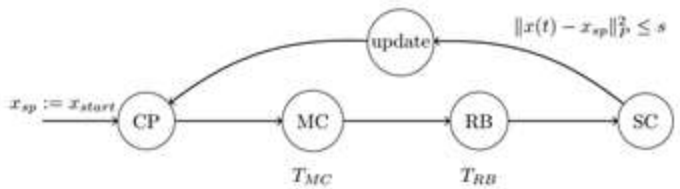
4 - Conclusions



Cyber

Physics



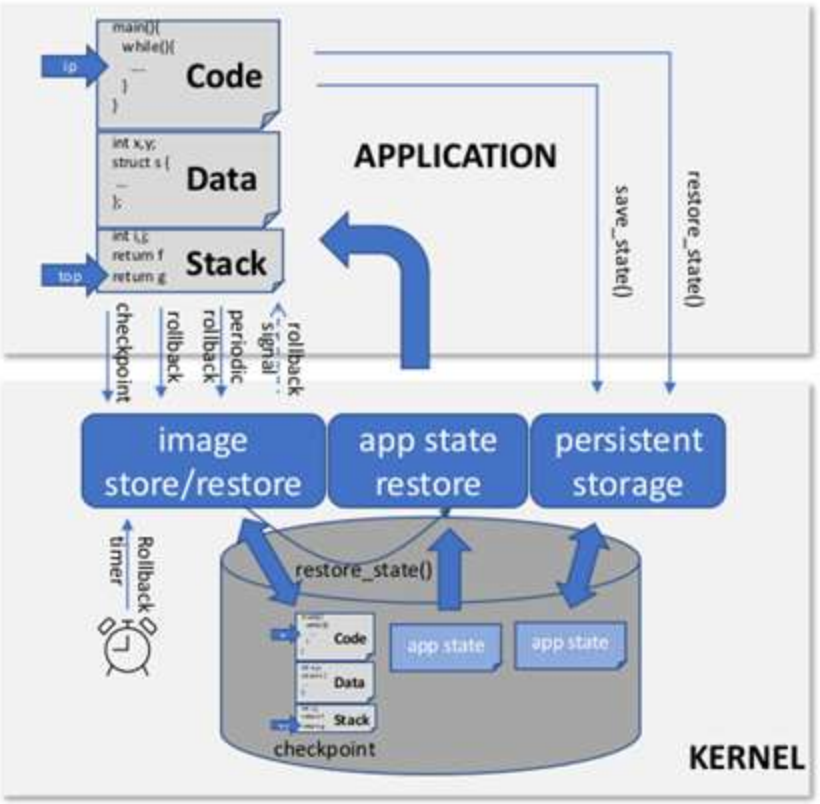


Romagnoli R, Krogh B.H, DeNiz D, Hristozov A.D, Sinopoli B. (2023). Runtime System Support for CPS Software Rejuvenation. IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, ISSN: 2168-6750, doi: 10.1109/TETC.2023.3267899

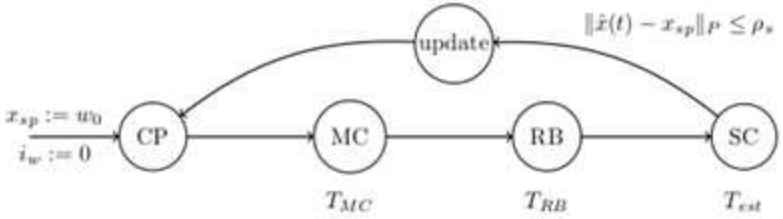
© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

4 - Implementation



- Application vs Kernel level



- `rollback_handler()`

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Safety Analysis

- State of the system

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

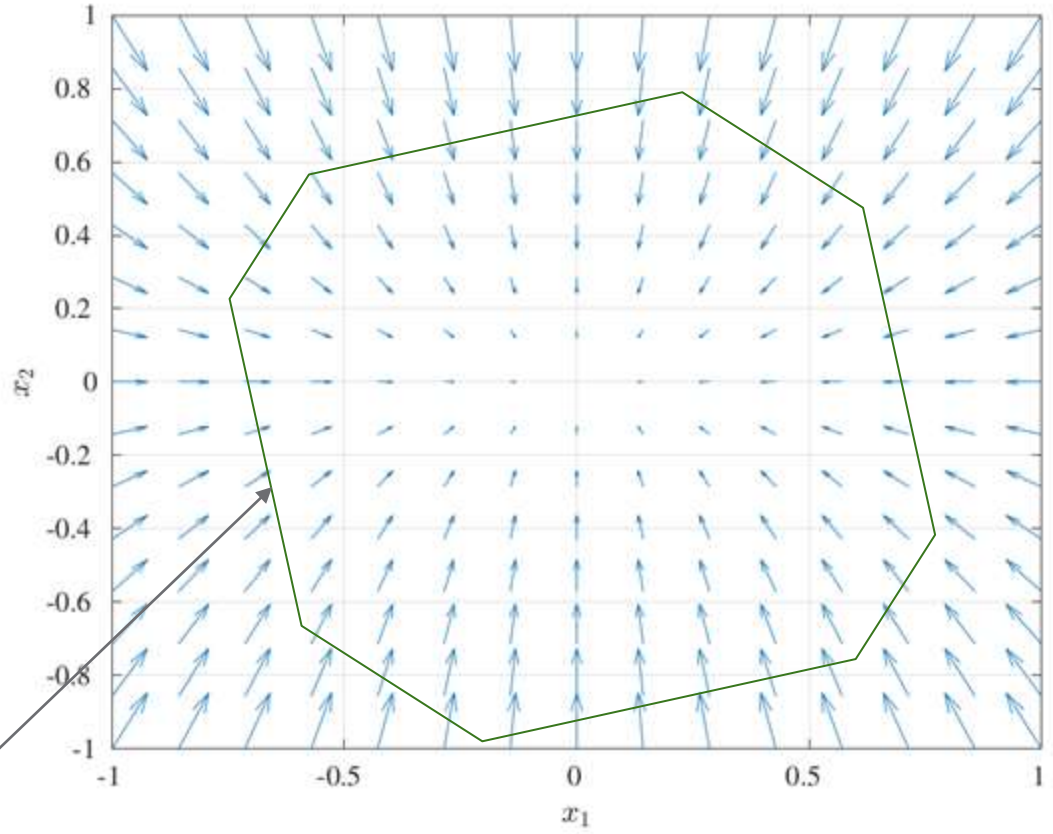
- Vector field

$$f(x) = \begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix}$$

- Dynamical system

$$\dot{x} = f(x)$$

Positively Invariant



© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Safety Analysis

6 DOF drone, the state has 12 components

- State of the system

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

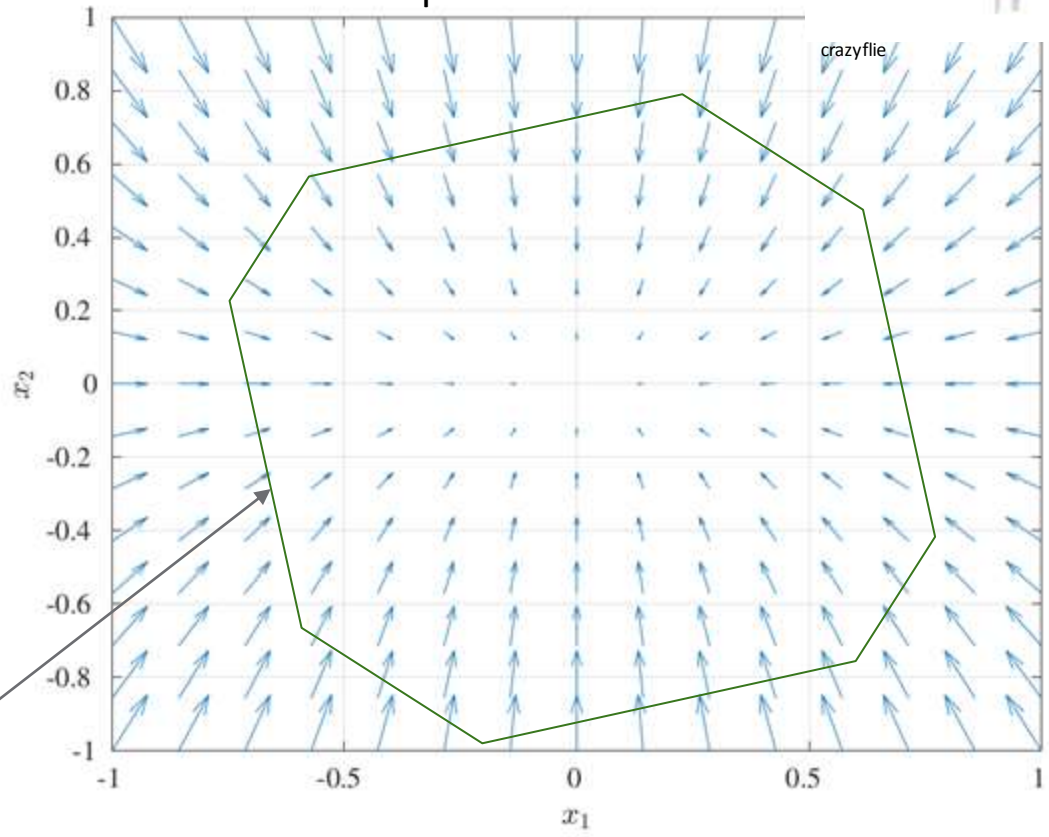
- Vector field

$$f(x) = \begin{bmatrix} f_1(x) \\ f_2(x) \end{bmatrix}$$

- Dynamical system

$$\dot{x} = f(x)$$

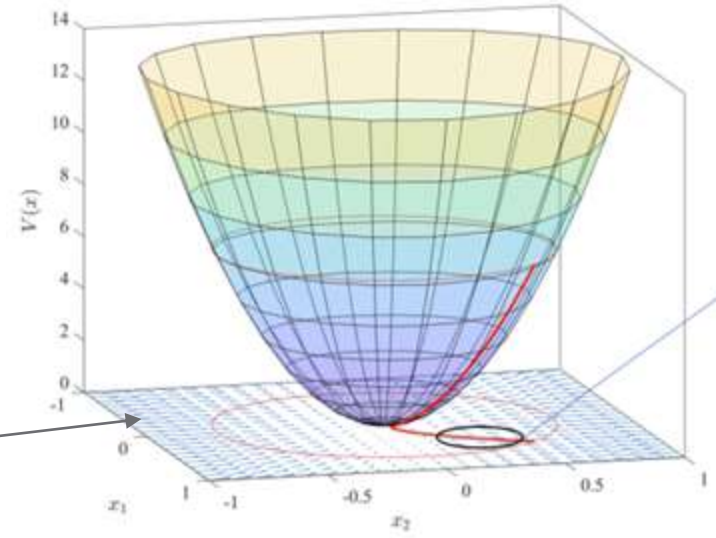
Positively Invariant



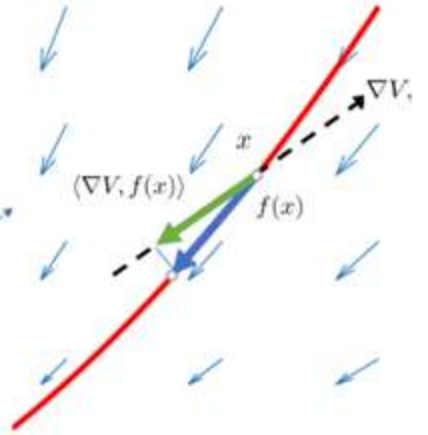
© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Software Rejuvenation Safety



$\dot{x} = f(x)$



Lyapunov level set

$$\Omega_c = \{x \in D \mid V(x) \leq c\}$$

Positively Invariant

Linear Systems $\dot{x} = f(x) = Ax$

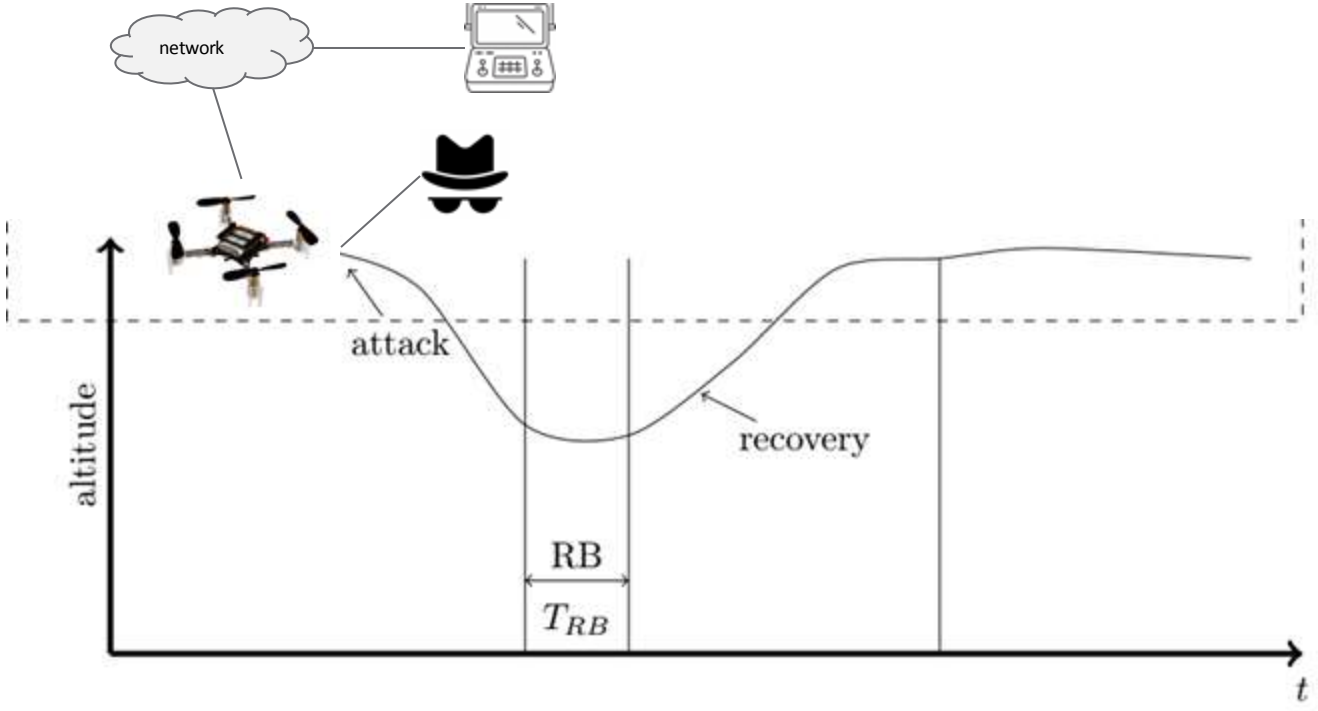
$$V(x) = x^T P x$$

$$\mathcal{E}_c = \{x \in D \mid x^T P x \leq c\}$$ Ellipsoid

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Example: Drone Hovering



Software Rejuvenation

Mission

- Hovering

Communication

- Connected to the network
  - PX4 : Mavlink

Cyber attacks

- On the run-time code

Idea

- **Software Reset/ Rollback**

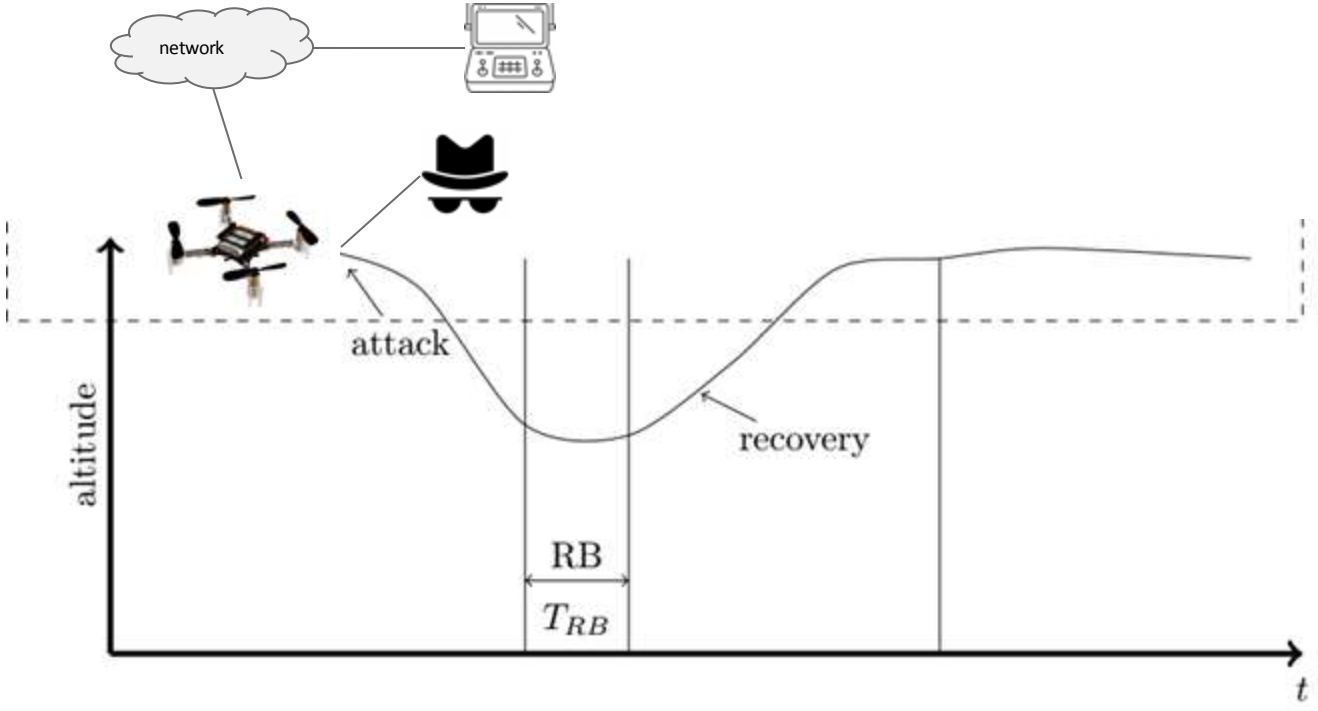
★ Periodic Reboot
★ On-line Reach set analysis

➔ Trajectory Tracking
➔ Full information (state) is not available

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Example: Drone Hovering



- Hovering
- Connected to the network
  - PX4 : Mavlink
- Cyber attacks on the run-time code
- Software Refresh

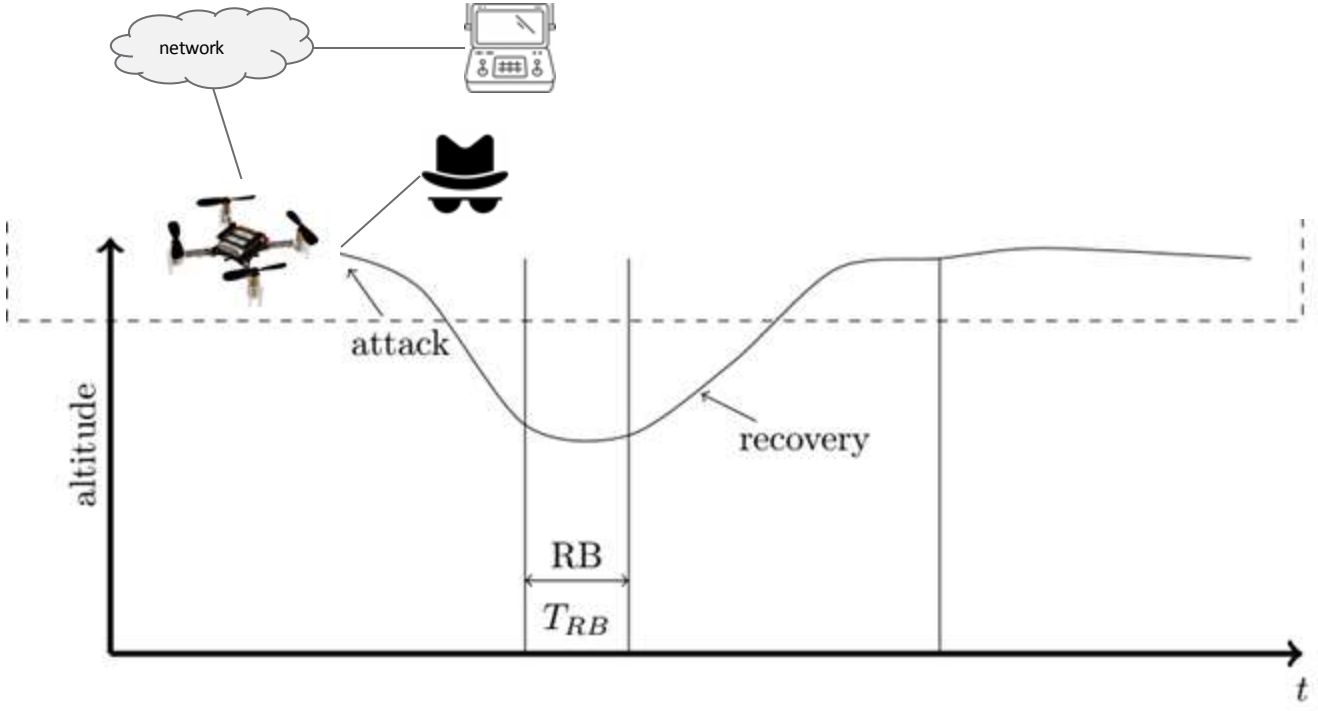
★ Periodic Reboot
★ On-line Reach set analysis

➔ Trajectory Tracking
➔ Full information (state) is not available

Software Rejuvenation

© 2023 Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution.

Proposed Software Rejuvenation Scheme



Software Rejuvenation

- Hovering
- Connected to the network
  - PX4 : Mavlink
- Cyber attacks on the run-time code
- Software Refresh

★ Periodic Reboot
★ On-line Reach set analysis

➔ Trajectory Tracking
➔ Full information (state) is not available

© 2023 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.