CERIAS

The Center for Education and Research in Information Assurance and Security

Risk Assessment of Multi-Agent System Under Denial-of-Service Cyberattacks Using Reachable Set Synthesis

Minhyun Cho, Sounghwan Hwang, and Inseok Hwang
(cho515, hwang214, kim4021, ihwang@purdue.edu)

Motivation

- **System Vulnerabilities of Multi-Agent Systems against Cyberattacks**
  - Multi-agent systems (MASs) heavily rely on the communication between agents.
  - The heavy reliance of MASs on inter-agent communication can potentially lead to system vulnerabilities to cyber threats that hinder communication.

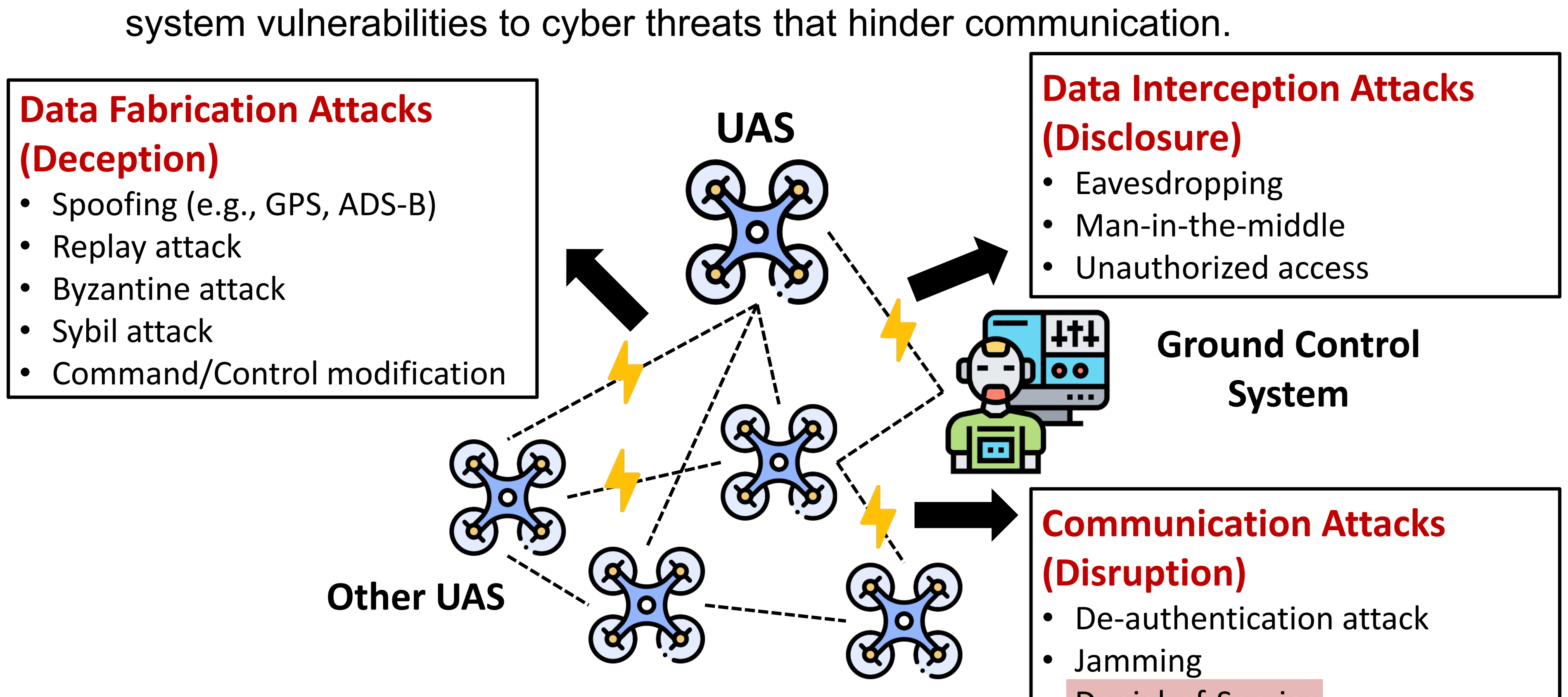

Figure 1. Various types of cyberattacks on MASs

- **Limitations of Previous Studies**
  - Counterattack strategies have been mainly using reactive approaches.
  - Operators or mission planners should assess associated risks and prevent a system from potential vulnerabilities in a proactive manner rather than naively applying robust control and using reactive strategies.
- **Objectives**
  - Propose a new proactive method to handle Denial-of-Service (DoS) cyberattacks.
  - Design a consensus control law and quantify the risk of DoS attacks on MASs.

Problem Formulation

- **Problem Statement**
  - DoS attacks can randomly disrupt the communication networks modeled, where the attacks are modeled as the Markovian process, i.e., the network topology randomly switches according to a specified transition probability.
  - To make realistic attack scenarios, we assume that the entries of the transition probability matrix, Ψ, are partially known.
  - A virtual leader-following distributed control protocol with bounded but time-varying delay, $0 < d_1 \leq d(k) \leq d_2$, is assumed.

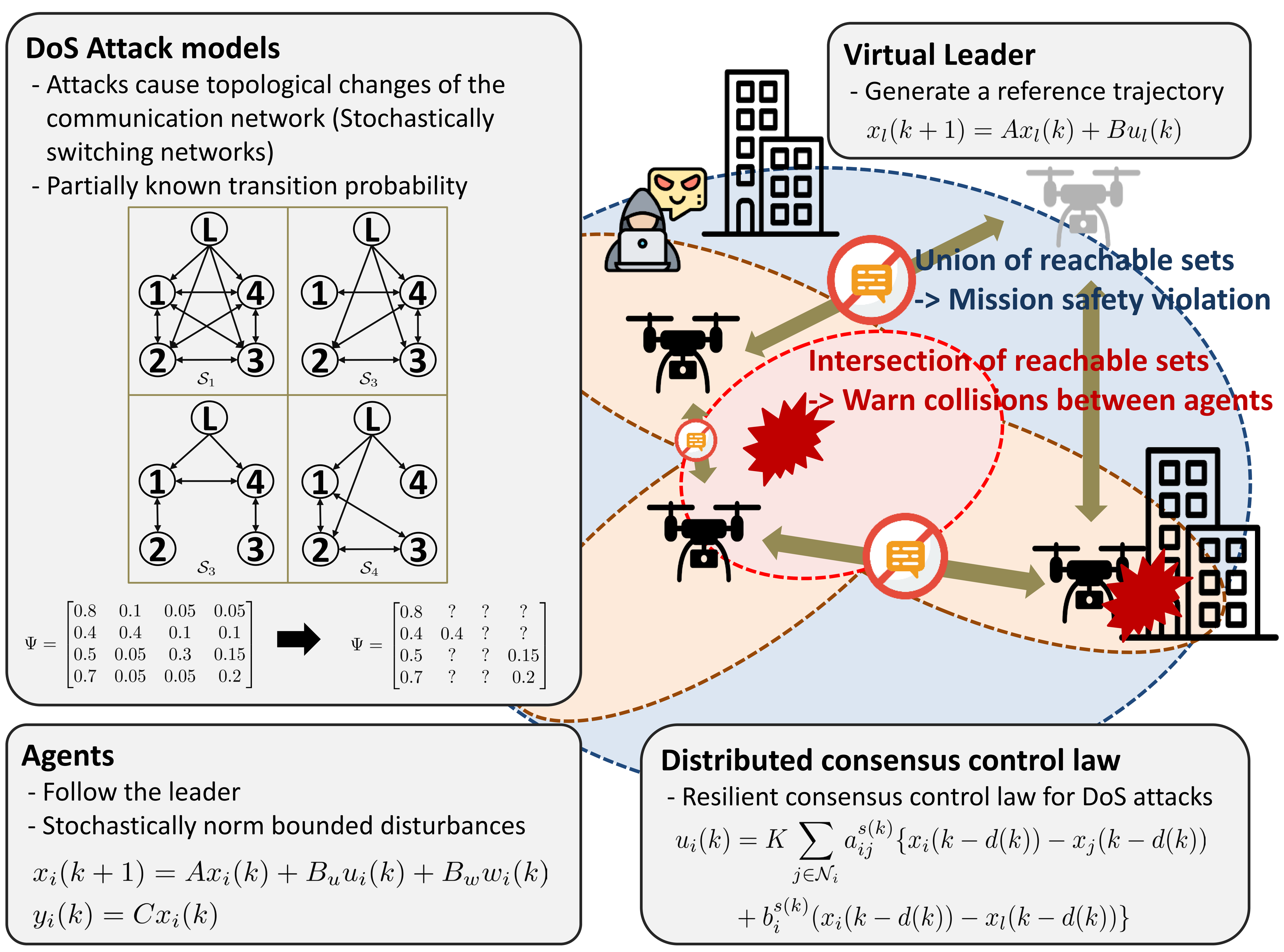

Figure 2. A schematic showing the structure of the MAS (w/ formulation) and potential risks associated with the MAS under DoS cyberattacks.

Main Results

- **Stabilization under DoS attacks**
  - From the equations given in the problem formulation section, we can obtain:
    $e(k+1) = (I_N \otimes A)e(k) - (\mathcal{L}_{s(k)} \otimes BK)e(k-d(k)) + (I_N \otimes B_w)w(k), \quad (1)$
  - A distributed consensus gain K that stabilizes the error dynamics (1), i.e., yields the bound error of the MAS $z(k) = (I_N \otimes C)e(k)$ with the bounded disturbance $w(k)$

$$\lim_{k \to \infty} \frac{\mathbb{E}\left[\sum_{\tau=0}^{k} ||(I_N \otimes C)e(\tau)||^2\right]}{\mathbb{E}\left[\sum_{\tau=0}^{k} ||w(\tau)||^2\right]} \leq \gamma^2 \quad (H_\infty\text{-criterion})$$

- **Reachable set computation for Markov switching system**
  - Compute ellipsoidal over-approximated reachable sets of the switching error dynamics (1) following Markov process
  - Project the error ellipsoids to the agents and quantify the risks at the agent and system levels using geometric operations, i.e., the union and intersections
- **Theorems**

Theorem 1 *For given $d_2 \geq d_1 \in \mathbb{R}^+$, consider the MAS error dynamics (1) under DoS attacks with time-varying delays. For given $\gamma \in \mathbb{R}^+$, if there exist proper matrices $G \in \mathbb{R}^{n \times n}$, $\hat{K} \in \mathbb{R}^{m \times n}$, $\hat{P}_\alpha = \hat{P}_\alpha^T \in \mathbb{R}^{n \times n}$ for $\alpha \in \mathcal{I}_{\mathbb{S}}$, $\mathcal{X}_i, \mathcal{Q}_i, \mathcal{Y}_i \in \mathbb{R}^{n \times n}$ for $i \in \mathcal{I}_3$, and $\mathcal{Z}_i, \mathcal{S}_i, \mathcal{M}_i, \mathcal{U}_i \in \mathbb{R}^{n \times n}$ for $i \in \mathcal{I}_2$, such that the following LMIs are satisfied for $\forall \alpha, \beta \in \mathcal{I}_{\mathbb{S}}$; then the distributed controller gain K can be determined, where $K = \hat{K}G^{-1}$. Finally, the MAS closed-loop error dynamics is stochastically mean-square stable with the H_∞ criterion.*

$$\Gamma_{\alpha\beta} < 0, \; \hat{P}_\alpha > 0, \; \text{and } \Phi_i > 0, \forall i \in \mathcal{I}_3,$$

where descriptions for the matrices are provided in the paper.

Theorem 2 *Let the LMIs from Theorem 1 be satisfied. For given $d_2 \geq d_1 \in \mathbb{Z}^+$, $\delta > 0$, and $\rho \in (0,1)$, if there exist matrices $P_\alpha \in \mathbb{R}^{Nn \times Nn} > 0$ and $\bar{P}_\alpha \in \mathbb{R}^{3Nn \times 3Nn} > 0$ for $\alpha \in \mathcal{C}(= \mathcal{I}_{\mathbb{S}})$, $Q_i \in \mathbb{R}^{Nn \times Nn} > 0$ for $i \in \mathcal{I}_3$, $S_i \in \mathbb{R}^{Nn \times Nn} > 0$ and $\bar{R}_i \in \mathbb{R}^{2Nn \times 2n} > 0$ for $i \in \mathcal{I}_2$, $Z_i = Z_i^T \in \mathbb{R}^{Nn \times Nn}$ for $i \in \mathcal{I}_3$, $Z_4 \in \mathbb{R}^{Nn \times Nn}$, $\bar{X} \in \mathbb{R}^{2Nn \times 2Nn}$, $\Theta \in \mathbb{R}^{2nN \times \kappa N}$ and $\bar{M}_\alpha \in \mathbb{R}^{\kappa N \times \kappa N}$ such that the following LMIs are satisfied:*

$$\bar{\Upsilon}_1, \bar{\Upsilon}_2 < 0, \mathcal{R}_1, \mathcal{R}_2 > 0, Z_2 - Z_3 > 0,$$
$$W_{P1\alpha}^T \bar{P}_\beta W_{P1\alpha} - \bar{M}_\alpha < 0, \; \forall \alpha \in \mathcal{C}, \forall \beta \in \mathcal{C}_{\mathbb{UA}}^\alpha,$$
$$\begin{bmatrix} S_2 & Z_4 \\ * & S_2 \end{bmatrix} > 0, \; \bar{P}_\alpha - \begin{bmatrix} P_\alpha & \mathbf{0} \\ * & \mathbf{0} \end{bmatrix} > 0, \; \kappa = (7n+p)N,$$

then the reachable set of MAS error dynamics (1) under DoS attacks with the Markovian process is bounded in mean-square sense. The detailed descriptions are provided in the paper.

Illustrative Example

- **Results**
  - Our method proposes an affordable way to evaluate the risk by using the reachable sets and geometric operations among the sets.
  - The union (blue) of the projected over-approximated reachable sets of the DoS-attacked case is larger than that of the attack-free case for every time instance.
  - In the attack-free case, the summation of the area of the intersection ellipses (red) at t = 18s is computed as 32.68m^2, while that of the attacked case is computed as 72.79m^2. The intersection reachable sets increase over two times, which reveals an increased probability of inter-agent collisions.

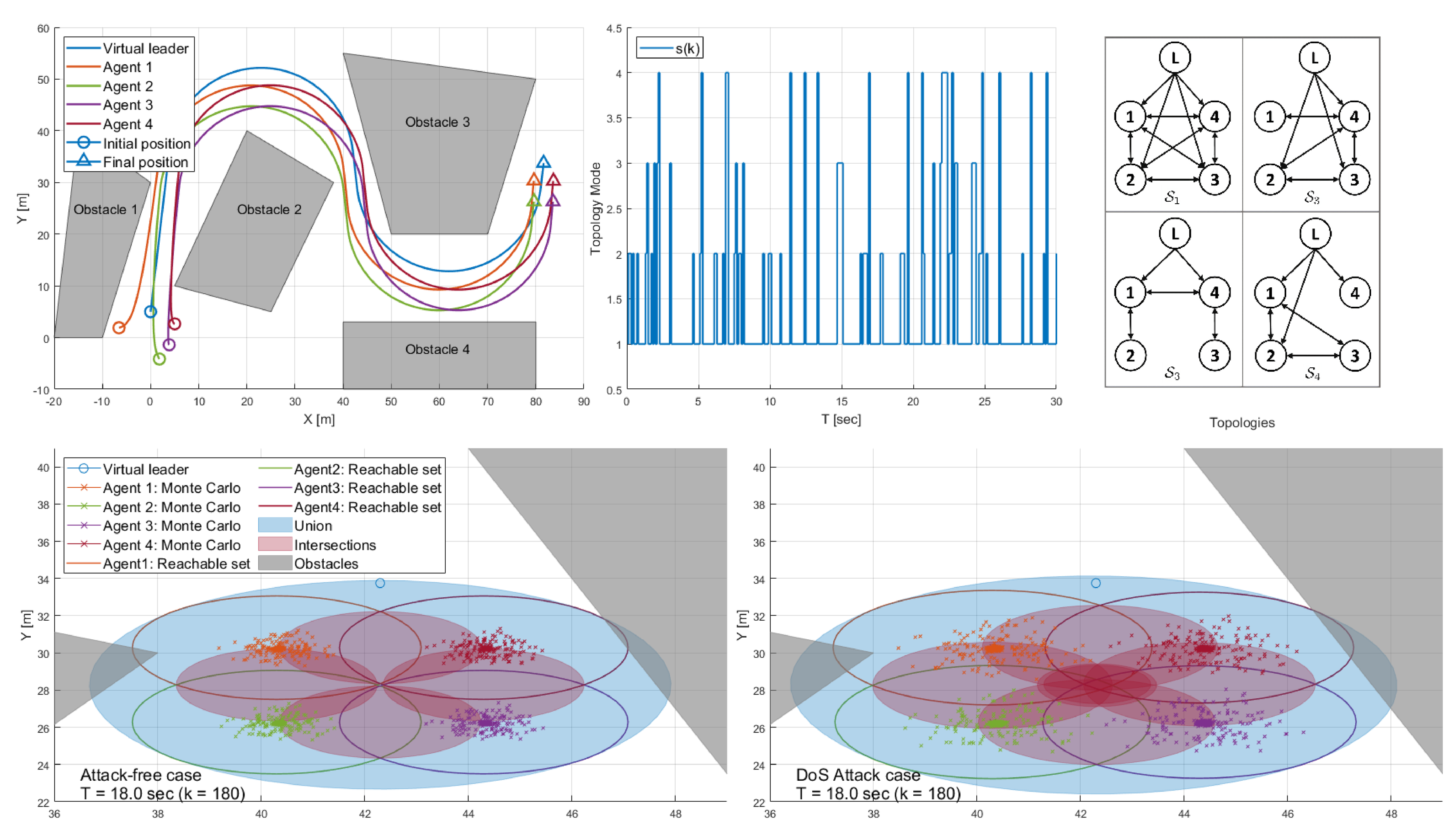

Fig 3. Trajectory of MAS (top left); network topology change in DoS attack case (top middle); network topologies (top right); over-approximated reachable sets at t = 18s in attack-free case (bottom left) and in DoS attack case (bottom right).

References

1. M., Cho, S., Hwang, I., Hwang, "Risk Assessment of Multi-Agent System Under Denial-of-Service Cyberattacks Using Reachable Set Synthesis", 2024 American Control Conference, Accepted.
2. S., Hwang, M., Cho, S., Kim, I., Hwang, "An LMI-based Risk Assessment of Leader-Follower Multi-Agent System under Stealthy Cyberattacks", IEEE Control Systems Letters, 2023.

PURDUE UNIVERSITY

CERIAS