CERIAS

The Center for Education and Research in Information Assurance and Security

An LMI-based Risk Assessment of Leader-Follower Multi-Agent System under Stealthy Cyberattacks

Sounghwan Hwang, Minhyun Cho, Sungoo Kim and Inseok Hwang

Motivation

- System Vulnerabilities of Multi-Agent Systems against Cyberattacks
  - Multi-agent systems (MASs) heavily rely on the communication between agents.
  - Cyberattacks can cause detrimental situations, such as crashes and collisions between agents, by disrupting the network of MASs.

Fig 1. Possible detrimental scenarios in the presence of cyberattacks

- Main Research Areas on the Cyber Security of MAS

	Attack Mitigation	Attack Detection
Goal	Offset the impact of cyberattacks using distributed/resilient control law	Detect abnormal behaviors induced by cyberattacks using detectors
Tools	Event-triggered control Observer-based adaptive control	Model-based detector (Kalman filter-based detector)

- Limitations of Previous Studies
  - Counterattack strategies discussed mostly coped with reactive approaches.
  - Reactive strategies might fail to protect MASs against sophisticated cyberattacks of which attackers can hide their strategies by bypassing detection mechanisms.
- Study Objective
  - Propose a new proactive method to handle stealthy cyberattacks.
  - Quantify the risks associated with stealthy attacks against MASs.

Problem Formulation

- Problem Statement
  - Stealthy cyberattacks can sneak into MASs without triggering the alarm of a residual-based attack detector which is widely adopted for various systems.
  - Stealthy cyberattacks can disrupt the system by inducing collisions between the agents or causing safety violations, which can be achieved by enlarging the reachable set of each agent using stealthy cyberattacks.

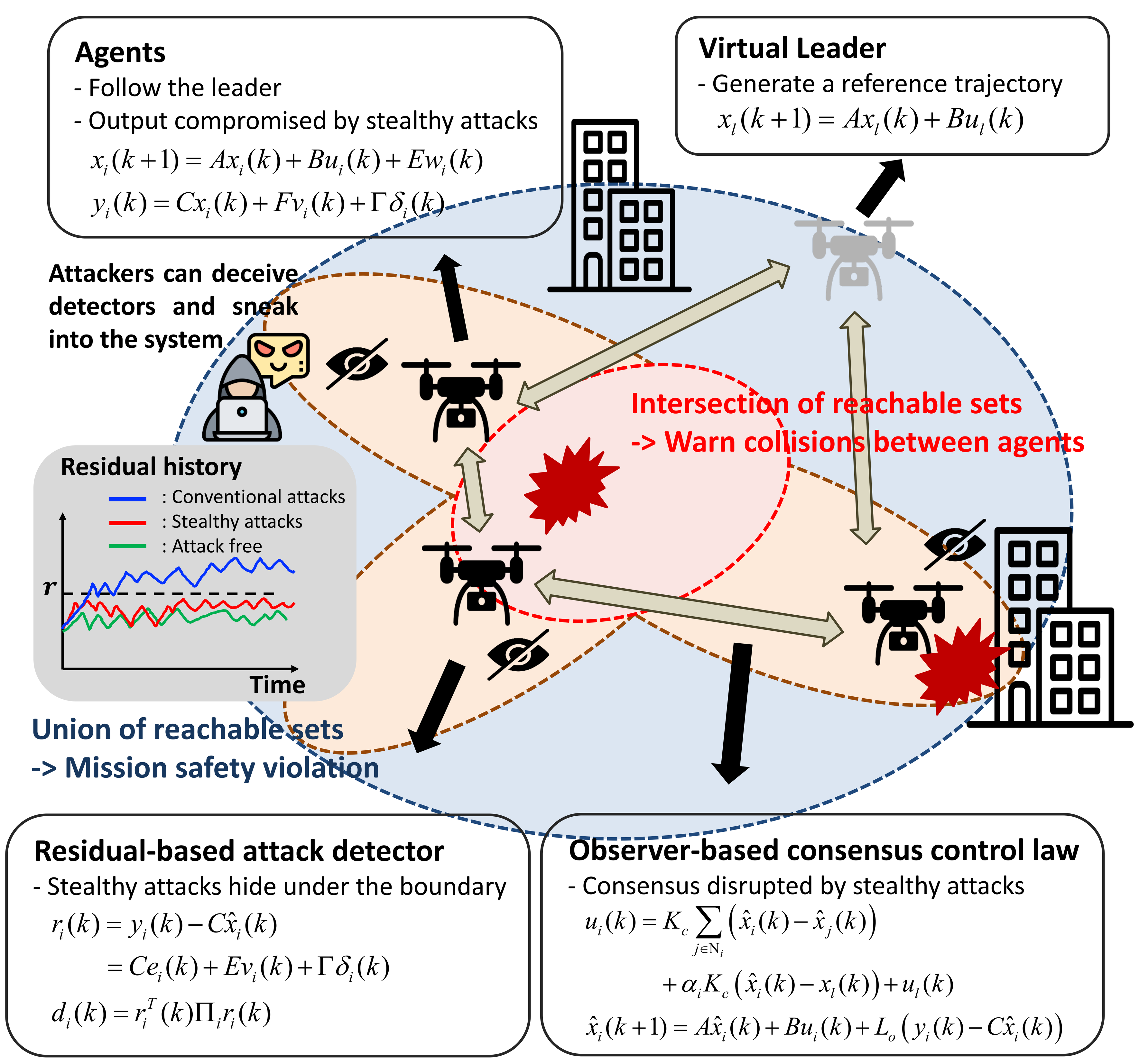

Fig 2. A schematic showing the structure of the MAS and potential risks associated with the MAS under cyberattacks

Main Results

Design Preliminaries
- Consensus control law design (Controller/Observer control gain)
- Residual-based attack detector design (Estimation error boundary, Minimum detection boundary)

Risk Assessment
- Compute ellipsoidal over-approximated reachable sets of agents in the MAS
- Quantify the risks of the MAS at the agent and system levels using geometric operations, the union and intersections, of the ellipsoids

Theorem (Computing the ellipsoidal over-approximated reachable set [2])

Consider a discrete linear time invariant system (1) with N peak-bounded perturbations:

$$x(k+1)=Ax(k)+\sum_{i=1}^{N}B_i w_i(k) \quad \text{where} \quad k\in\mathbb{Z}^+,\ i\in\mathbb{N},\ x\in\mathbb{R}^n,\ A\in\mathbb{R}^{n\times n},\ B_i\in\mathbb{R}^{n\times m},\ w_i^T(k)W_i w_i(k)\le 1$$

and the reachable set R_x^k at time step k from the initial state $x(1)$ is defined as follows:

$$R_x^k=\left\{x(k)\mid A^{k-1}x(1)+\sum_{i=1}^{N}\sum_{j=0}^{k-2}A^jB_iw_i(k-1-j)\right\}$$ (= A set of states reachable in $\mathbb{R}^n$ within k steps)

Then, R_x^k satisfies $R_x^k\subseteq\varepsilon_k^x=\left\{x(k)\mid x^T(k)Px(k)\le a_k^x\right\}$ if there exists a solution for the following LMI-based optimization for a given parameter $a\in(0,1)$:

$$\min_{P,a_1,a_2,\cdots,a_N} -\log(\det P) \quad \longrightarrow \quad a_k^x=a^{k-1}x^T(1)Px(1)+\frac{N-a}{1-a}(1-a^{k-1})$$

$$\text{s.t. } a_1,a_2,\cdots,a_N\in(0,1),\ P=P^T>0,\ a_1+a_2+\cdots+a_N\ge a,$$

$$\begin{bmatrix} aP & * & * \\ PA & P & * \\ \mathbf{0} & B_D^TP & W \end{bmatrix}\ge 0,\ W=\begin{bmatrix}(1-a_1)W_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & (1-a_N)W_N\end{bmatrix},\ B_D=\begin{bmatrix}B_1 & B_2 & \cdots & B_N\end{bmatrix}$$

Illustrative Example

- Results
  - The leader-following agents in a given MAS achieve a mission without safety violations when no stealthy attacks are engaged.
  - The union (blue) of the projected ellipsoidal over-approximated reachable sets of the stealthy-attack case is larger than that of the attack-free case for all given time instances.
  - The intersections (red) of the reachable sets of three agents increases over the simulation time, which means an increased probability of an inter-agent collision.

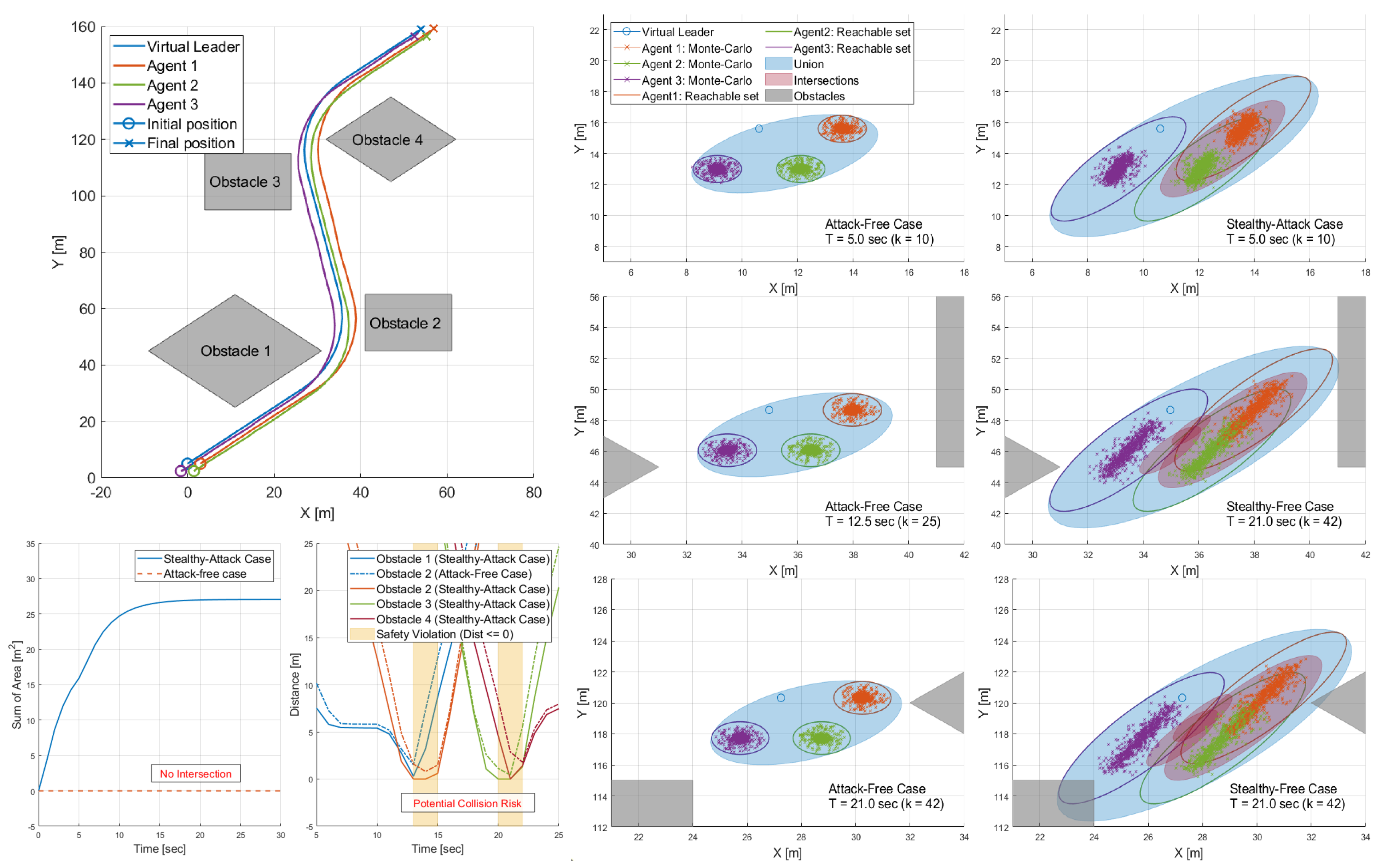

Fig 3. Formation control of a leader-follower MAS in the attack free-case (top-left); the ellipsoidal over-approximated reachable sets computed at three time instances (right); the sum of intersections and the minimum distance between the union and obstacles (bottom-left)

References

1. S., Hwang, M., Cho, S., Kim, I., Hwang, "An LMI-based Risk Assessment of Leader-Follower Multi-Agent System under Stealthy Cyberattacks", 62nd IEEE Conference on Decision and Control, Under Review.
2. M., Carlos, et al., "Security metrics and synthesis of secure control systems," *Automatica,* Vol. 115, 2020.

PURDUE UNIVERSITY

CERIAS