Future Intelligent Network System Laboratory

Jianping He

Shanghai Jiao Tong University

Email: jphe@sjtu.edu.cn

Group Homepage: https://iwin-fins.com/

IWIN Center: https://iwin.sjtu.edu.cn

Welcome to SJTU

招才引智：有意者欢迎发邮件至 jphe@sjtu.edu.cn

1）**课题组拟招收多名博士后研究员**。研究方向包括但不限于工业网络系统、优化与决策、机器学习与智能控制、网络系统安全、车联网大数据等方向。待遇丰厚，享受上海交通大学博士后福利待遇，表现突出者给予额外补贴。欢迎相关学科的优秀青年博士咨询。

2）**拟招收硕士研究生2-3名，博士研究生1-2名**。研究方向包括但不限于分布式安全隐私理论及应用、分布式学习与智能控制、机器人协同攻防系统及理论。欢迎校内外优秀本科生、研究生加入研究小组。组将提系统化的科研训练和国际化的平台。

3）**拟招收本科生3-5名**。包括本科毕业设计、PRP、莙政等科研训练项目。非常欢迎数学基础好、编程能力强、有意出国的本科生。表现突出者将推荐至美国、加拿大、香港等著名高校（如Harvard、UCSB、Waterloo、UVIC、HKUST）进行交流或继续深造。

欢迎加人IWIN-FINS LAB!

Outstanding students, beautiful and comfortable environment

课题组概况

IWIN-FINS

未来智能网络系统课题组 (FINS，Future Intelligent Network System Laboratory) 隶属于上海交通大学智能无线网络与协同控制中心 (IWIN-Center)，依托上海交通大学自动化系与系统控制与信息处理教育部重点实验室。

现有成员大都由各大高校Top 5%学生推免加入，包括清华、上交、西交、华科、华电等。现有博士后一人、博士六人、硕士及以下十人，另有多名毕业学生进入名校 (牛津大学、宾大、UCSB等)、名企(华为、TP-Link等)。课题组指导老师为何建平副教授。

操作台

实验台

办公室

FINS LAB is one of IWIN Research Group

We focus on developing distributed, secure and intelligent systems for mobile robots, machine learning, control and optimization

IWIN-FINS

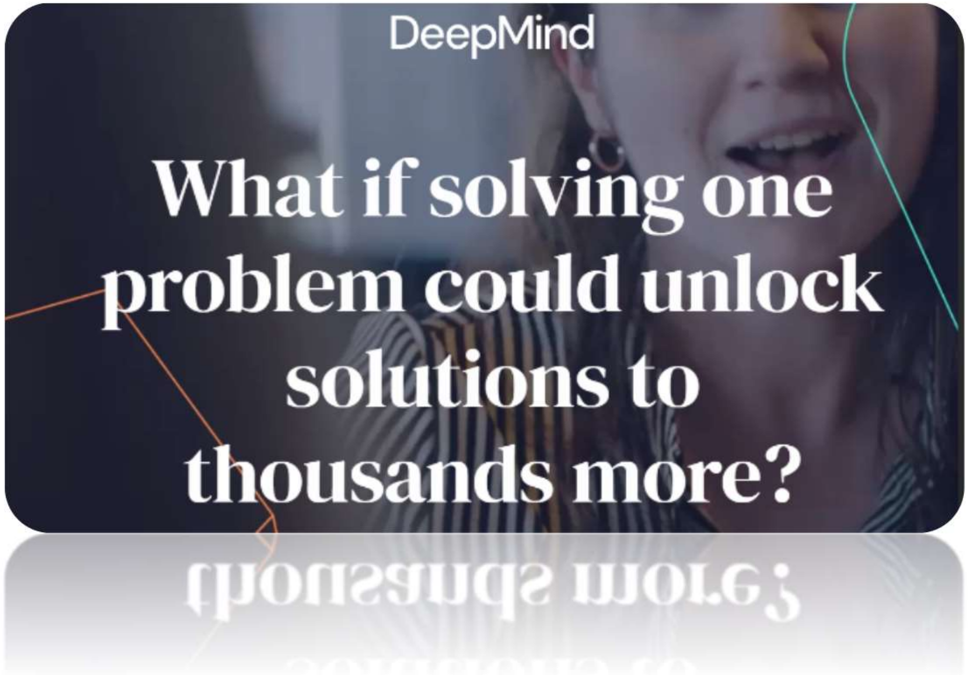
Team Concept

- From small questions to essence of things
- Seize every spark of splendid ideas in daily life

Confident

Competitive

Cooperative



Work, work hard

Play, play well

Embrace research and make your devotion worthy!

IWIN-FINS Group

Team Members

Research Direction

- **Secure Cooperation** → **Platform & System**, **Attack & Defense**, **Reinforce & Optimization**
- **Platform & System** → **Attack & Defense** → **Reinforce & Optimization**

Groups


Hardware Framework

Software Algorithm


Control Algorithm


Navigation Localization


Digital twins


Intelligent software


Intelligent Attack


Topology Inference


Active Learning


Concealed Collaboration


A-obstacle Avoidance


Reinforce learning


Coverage Detection

Non-convex Optimization


Fault-tolerant Control


Attack Compensation


Unpredictable Control


Learing algorithm

Goals

Learnable Robots
Soft-defined System

Learning Theory
Attack Algorithm
Secure Evaluation

Compensation and Reinforce
Dependable Optimization

IWIN-FINS Group

IWIN-FINS

Graduates & Alumni

刘聪
[毕业-华为]

廖文静
[毕业-hellobike]

缪洋
[毕业-TPlink]

孙明靖
[毕业-ASU]

马孟洲
[毕业-拼多多]

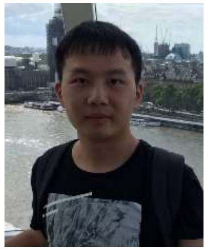
李鸿博
[SUTD]

蔡一凡
[UPenn]

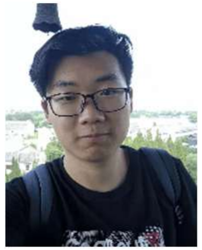
王汉
[Oxford]

毛祥宇
[清华]

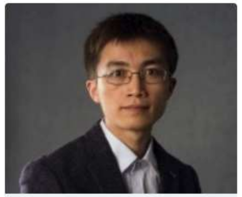
王亚蓉
[清华]



郑文喆
[北航]



杨大力
[交大]



Fei Tong
Southeast University
personal website

Chengcheng Zhao
University of Victoria
personal website

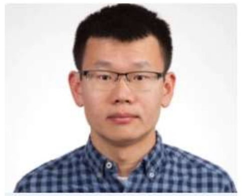
Xiaoming Duan
UC Santa Barbara
personal website

Jiayi Chen
University of Waterloo
personal website

Heng Li
Central South University

Xin Wang
Zhejiang University

Guanghui Wang
Henan University

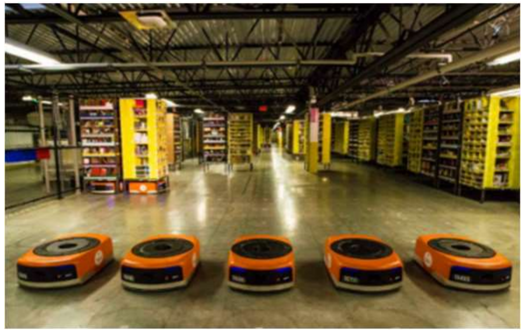


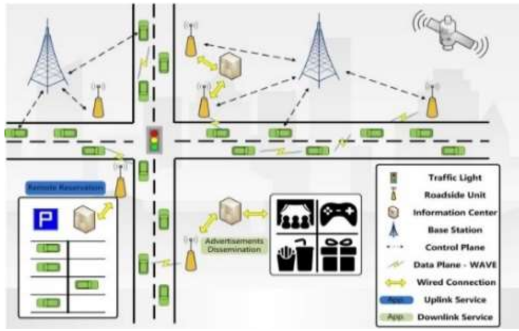
Yuanzhi Ni
Jiangnan University

Research Interests

IWIN-FINS

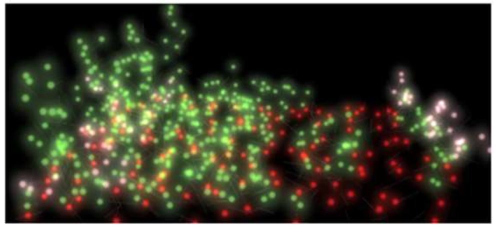
Network systems



We focus on developing distributed, secure and intelligent systems for mobile robots, machine learning, control and optimization

Intelligent Robot Control Systems



Secure Data-driven Cooperation

Coordinated Charging Systems

Multi-Agent Learning Systems

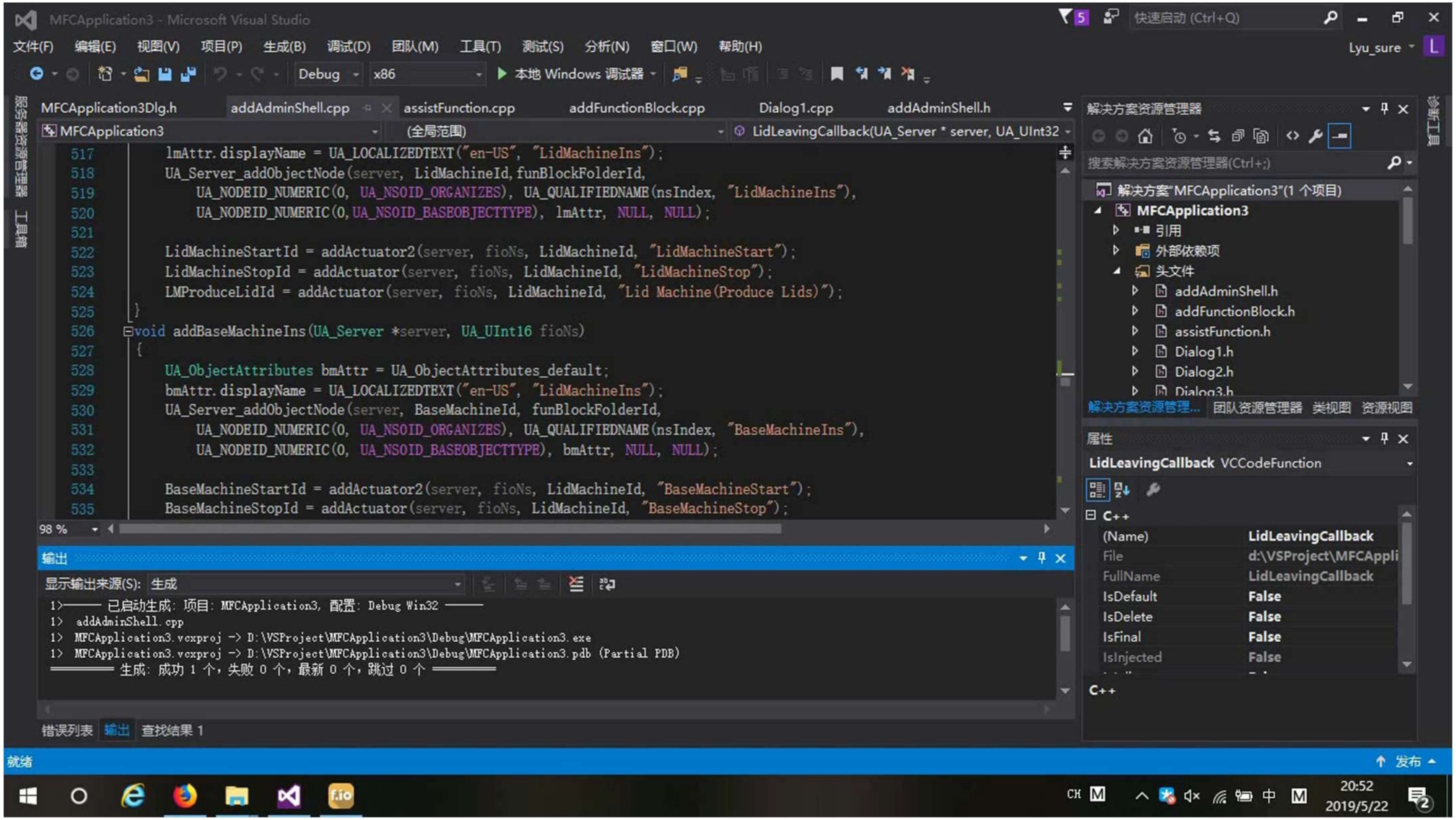
- Advanced robot structure design and control
- Robots cooperative attack and defense
- Robot distributed operation software and systems

- Independable information based secure control
- Analysis and modeling for data privacy preservation
- Data-driven model inference and optimization

Network + Cooperation: Distributed, Secure, Intelligent

IWIN-FINS

Integrated Information Model



Why Network and Cooperation

IWIN-FINS

What We Focus on?

Networking + Cooperation

Distributed Learning, Control and Optimization

1 + 1 > 2 and N+N >> 2N

Multi-robot Systems, Multi-agent Systems, Sensor Networks, Vehicular networks

What We Focus on?

IWIN-FINS

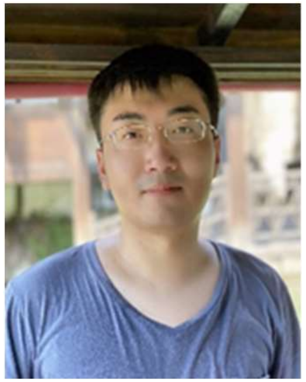
Intelligent Robot System Group

IWIN-FINS

Intelligent Robot Systems

We build a self-designed multi-robot platform, where the robots are capable of running in omni-direction with highly accurate control and reliable communication performance. Moreover, the robots are very convenient to embed other advanced on-board equipments to meet different kinds of practical application requirements.

- Advanced robot structure design and control
- Robots cooperative attack and defense
- Robot distributed operation software and systems



Xuda Ding, PhD

Hardware Framework

Hao Jiang, MS

Software Algorithm

Pengjie Fang, MS

Control Algorithm

Wanbin Han, MS

Navigation Localization

Chengye Liao, MS

Digital twins

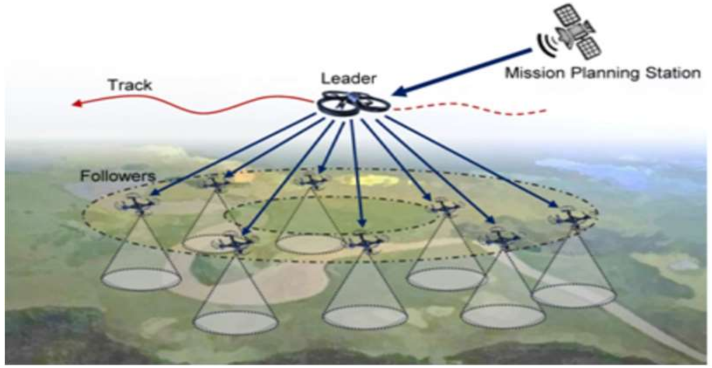
Haoxuan Pan, MS

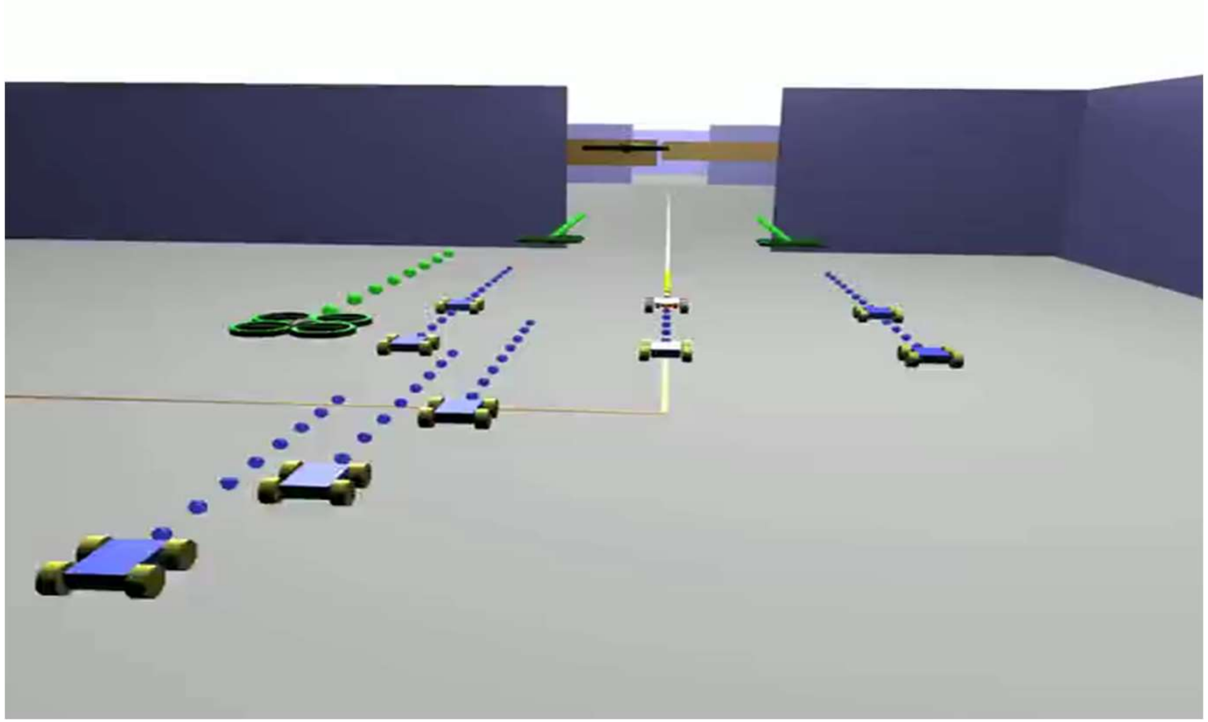
Intelligent software

Multi-robot Systems

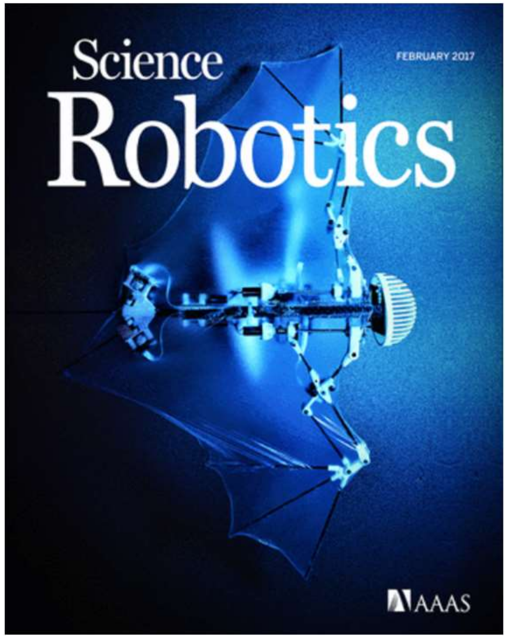
A system consisting of multiple robots, where the robots coordinate with each other to achieve well defined goals

- The ability of single robot is limited
- Cooperate to perform complicated tasks
- Strong ability of acquiring and processing information





https://www.youtube.com/results?search_query=Navigation%2C+localization+and+stabilization+of+formations+of+unmanned+aerial+and+ground+vehicles.



G.-Z. Yang, et al., The grand challenges of science robotics," Science Robotics. 3(14), (2018).

高性能移动机器人平台

兼容多种运动模式的高强度、易扩展、稳定可靠的机器人机械结构及其主控设计

机械结构

- 车体稳定触地的四轮独立悬挂设计
- 面向工业场景的高强度小尺寸结构设计
- 面向复杂场景的抗外损强化设计与防水防爆设计

硬件设计

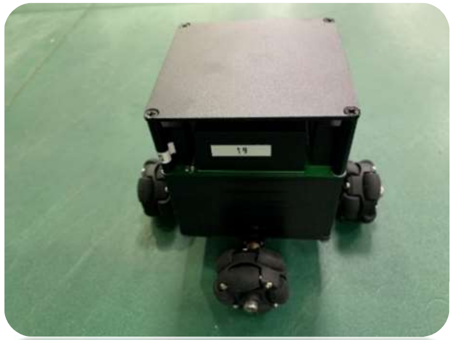
- 扩展多种传感器的模块化接口设计
- 电磁兼容、模数电分离等抗干扰设计
- 外设模插拔的通用接口设计
- 易损芯片的快速更换机制设计
- 兼容Arduino、MATLAB软件的单片机固件设计

机器人设计

IWIN-FINS

异构机器人设计

驱动方式：差分、全向；主控异构：8\32位单片机、ROS系统；多传感器、易扩展接口



V1 Mini化全向

V2 高承重越野

V3 抗外损强化

高度：100mm
半径：75mm
位移控制精度：±1cm
最大速度：40cm/s
续航时间：6h
适合群集控制

高度：180mm
半径：175mm
位移精度控制：±1cm
最大速度：147cm/s
无线通讯距离：100m载
重：7kg

自身控制闭环
核心独立封装
机械性能强悍
车身载重强化
四轮独立悬挂系统
扩展口灵活适配

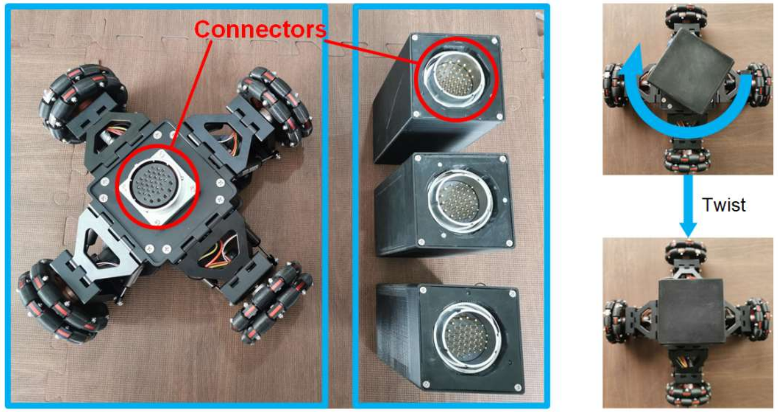
模块化设计 - 维护性高 模块编程易上手
全向/差速双模式控制 - 适用于多种场景

平台搭建

模块化设计：独立悬挂；电磁兼容/模数电分离抗干扰；抗外损与防水防爆

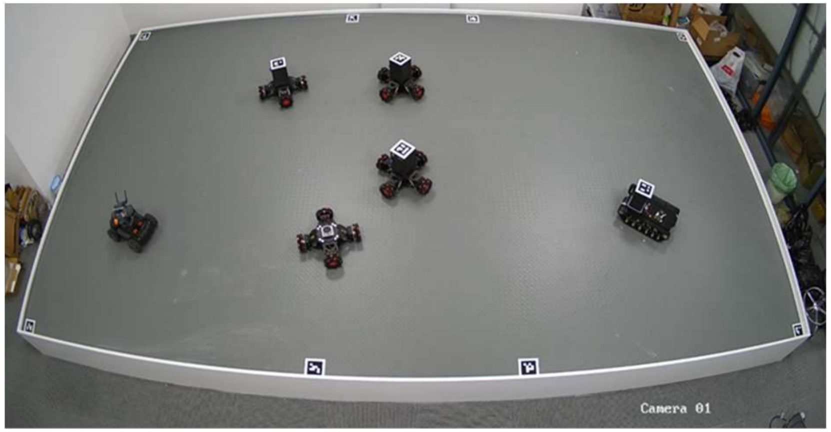
高可扩展性：接口灵活适配；兼容Arduino/MATLAB等软件；模块易更换接口和电路

可拆卸
模块连接

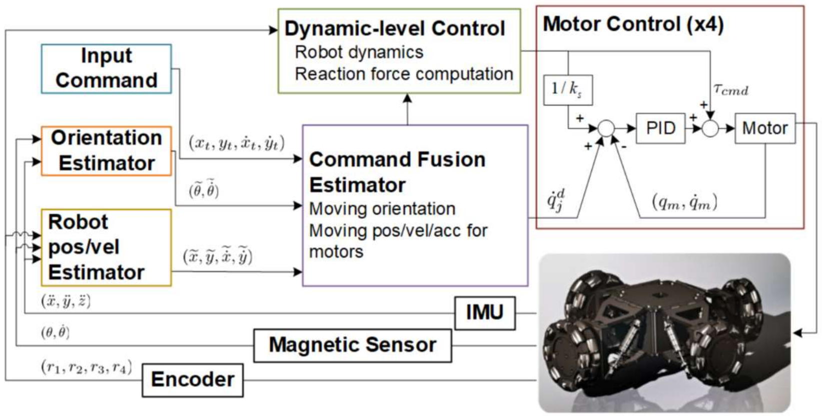


Robot chassis　　Controllers　　Connected

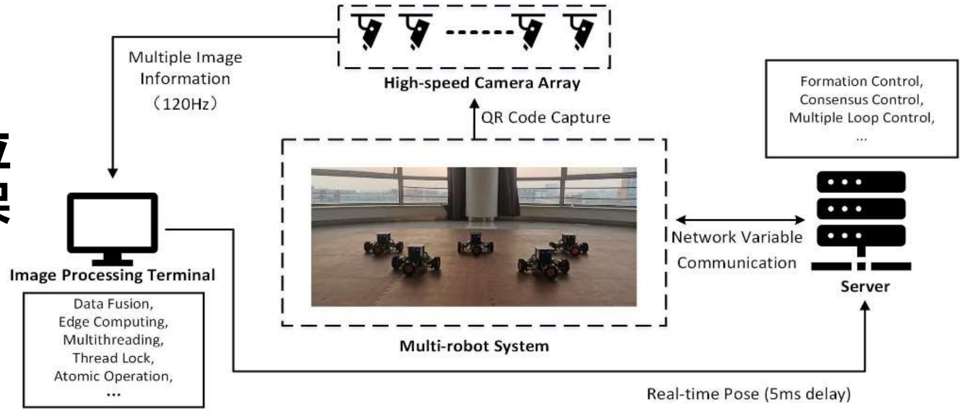
分布式
全局定位



控制
框架



定位
框架



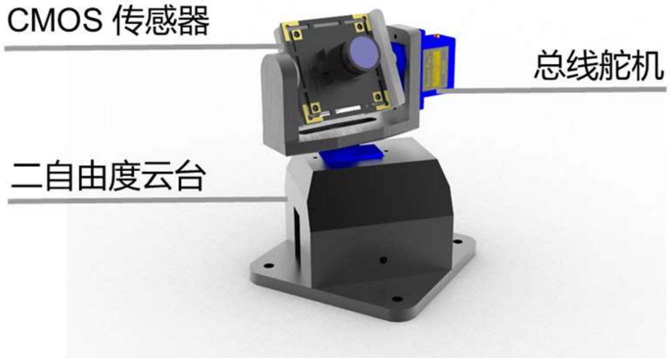
拓展性高、越野性强、运动模式灵活的全向自主智能机器人

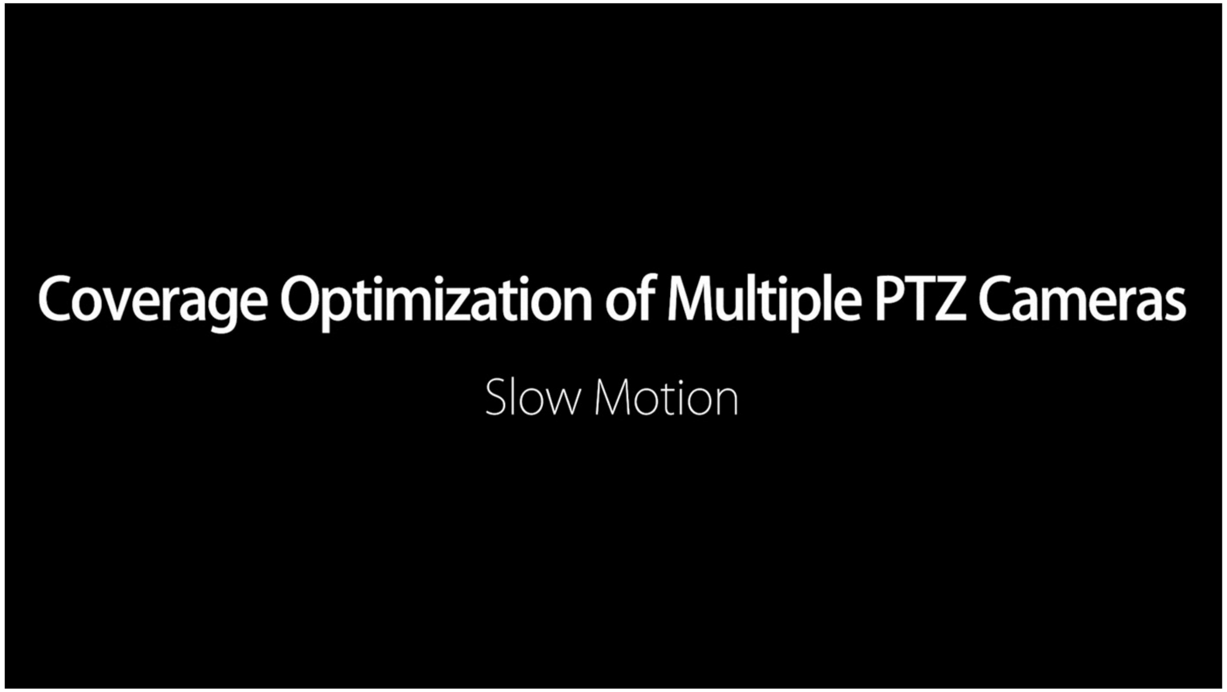
全局定位系统

IWIN-FINS

分布式摄像头阵列：体积小、部署方便、扩展性强、可靠性高

AprilTag 视觉基准系统：低像素、高精度、六自由度定位





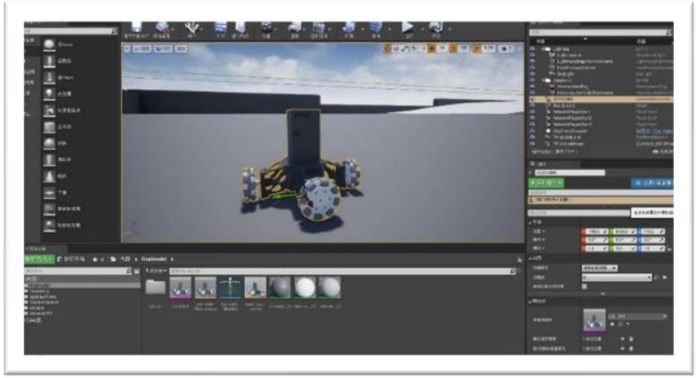
- 自适应阈值分割
- 查找轮廓
- 解码识别
- 坐标转换

面向分布式架构的云台相机结构、相机感知与覆盖自动校准

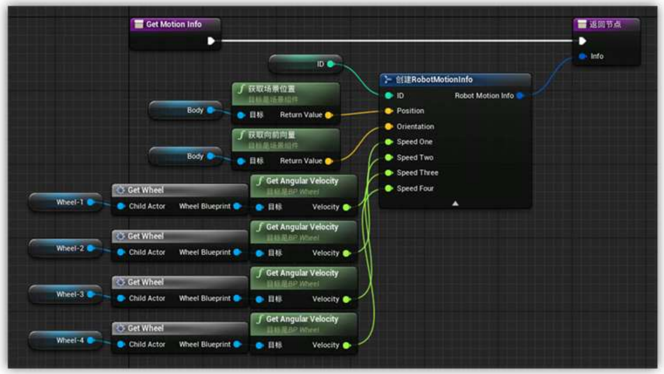
基于数字孪生的智能建模

IWIN-FINS

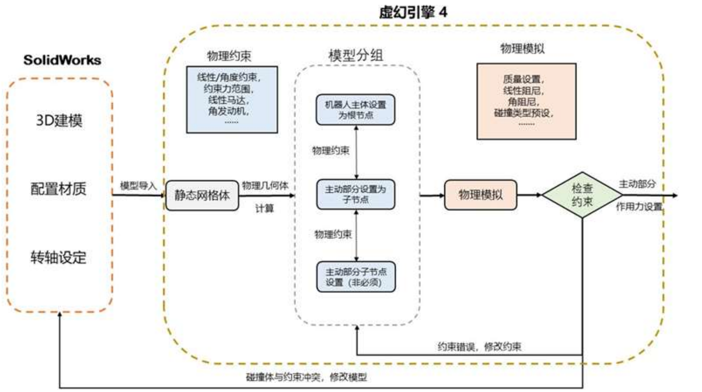
基于虚拟引擎4+Solid Works开发，建立孪生映射



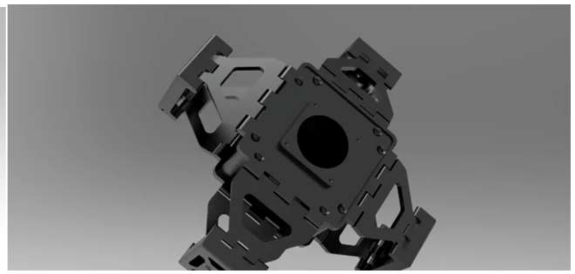
虚幻引擎调用



虚实接口构建



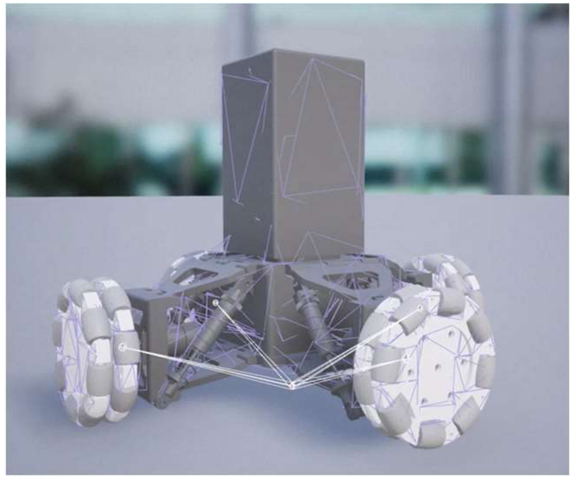
机器人模型配置



268个组件

五大零件组

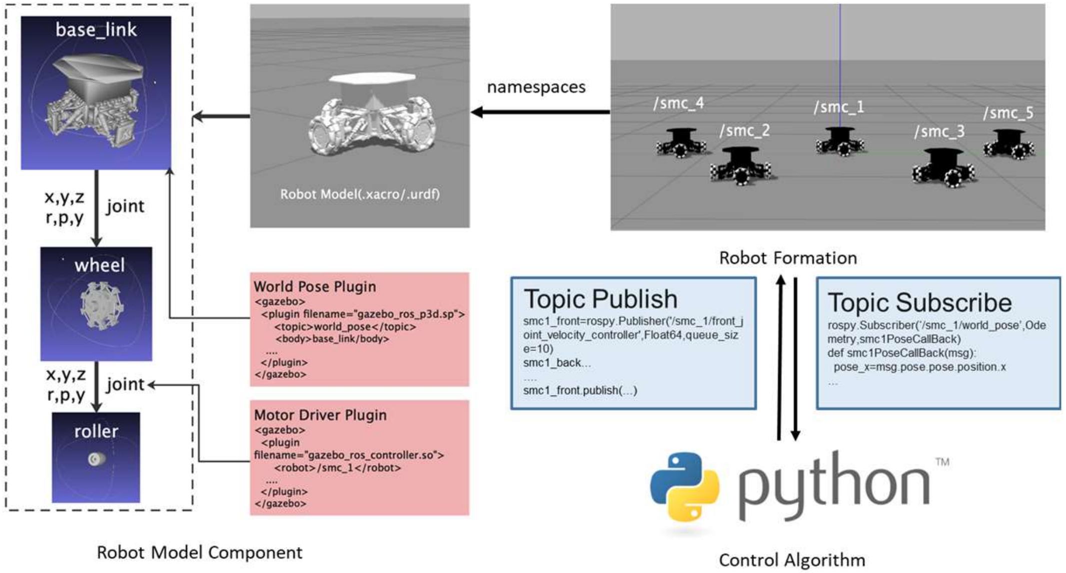
碰撞几何体
凸包分解
物理约束
代替连接轴

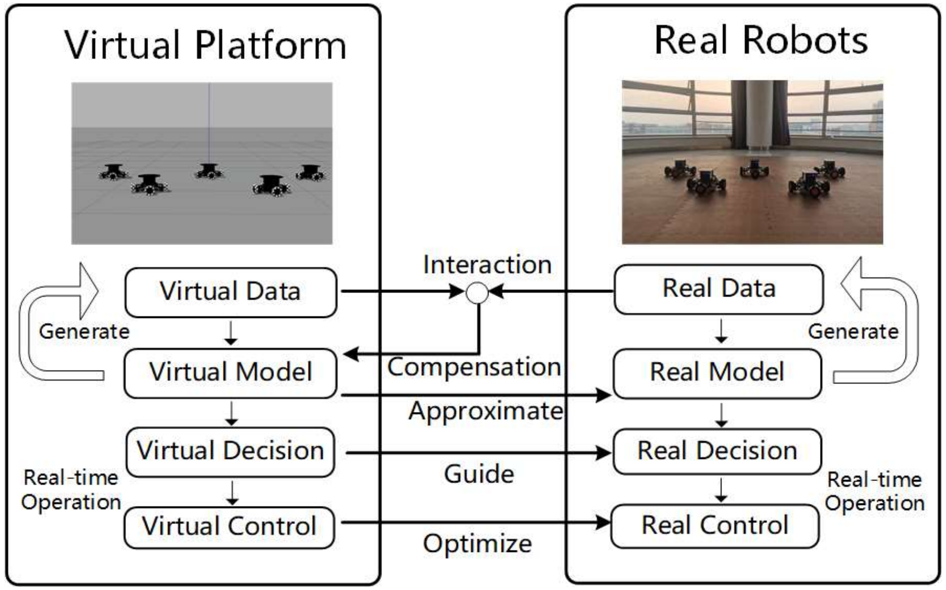


赋予孪生模型以实际物理意义、突破传统虚拟建模的可视化局限

智能协作控制框架

虚拟-物理双闭环的新型控制设计，环境与模型实时学习-反向优化





- 模块自主设计
- 精准映射建模
- 多编程语言并行
- 异构设备互兼容

基于ROS架构的虚拟建模

- 动态同步演化
- 实时状态监测
- 数据驱动学习
- 虚拟反馈闭环
- 系统模型修正
- 决策超前预测

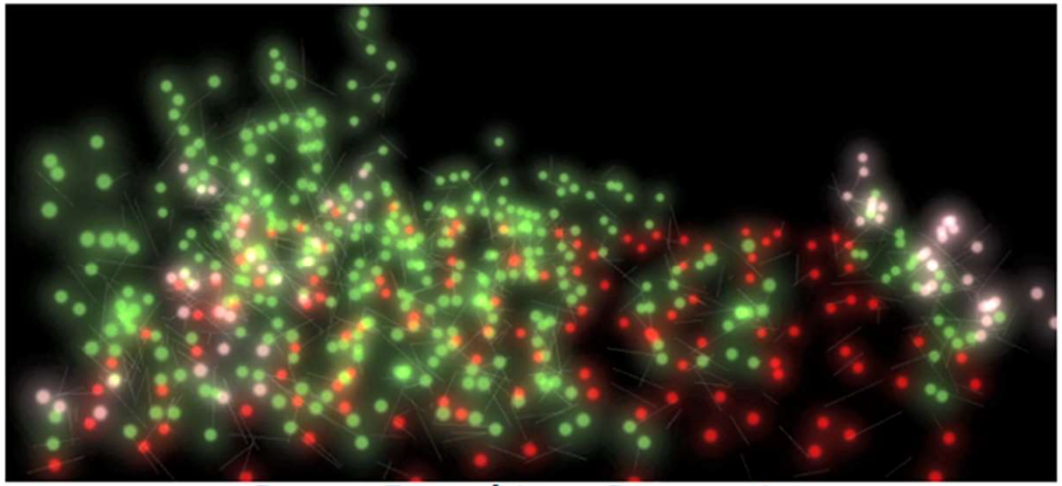
虚拟反馈下的控制优化设计

数据-机理双驱动建模、虚实互联的双闭环反馈优化机制

平台展示

Cooperation and Security in Network Systems

IWIN-FINS



Secure Data-driven Cooperation

Multi-agent cooperation has a mainstream in the field of control and receives considerable attention. Among its numerous applications, privacy and security concern arise wherever personally identifiable information is collected, stored, used or exhibited. The data of this process play a vital role for secure control. And we are dedicated to investigating the privacy-preserving information exchange mechanism and reliable control design to secure the system cooperation.

- Independable information based secure control
- Analysis and modeling for data privacy preservation
- Data-driven model inference and optimization

Yushan Li, PhD

Intelligent Attack

Qing Jiao, PhD

Topology Inference

Xiangyu Mao, PhD

Active Learning

Zitong Wang, PhD

Concealed Collaboration

Yarong Wang, MS

Path Planning

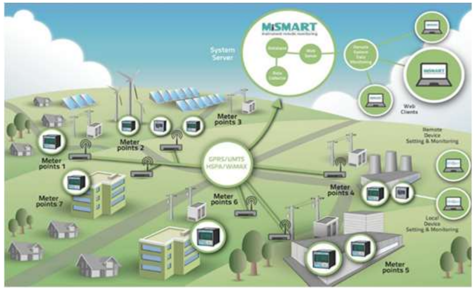
Chendi Qu, PhD

Reinforce learning

Cooperation of Network Systems

The network systems are composed of multiple agents

- Ability of local communication and computations
- Achieve global objectives via local interactions



Smart grid

Wireless sensor network

Social network

Robotics Swarms

The system interaction is critical for the whole operation performance

- Whether the system will be stable? How is the convergence performance

The interaction relationships can be modeled as a topology structure

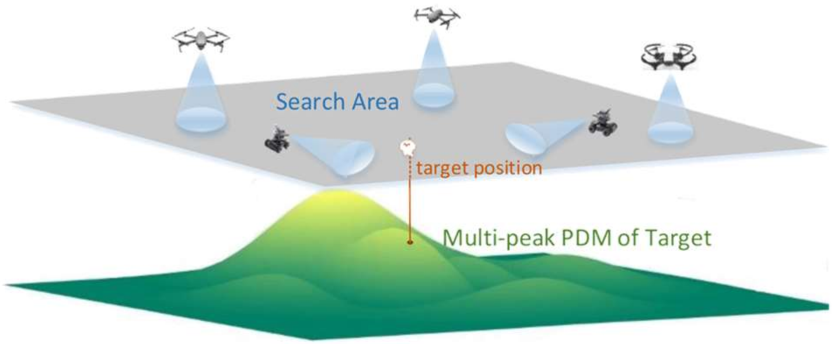
$$\text{Information interaction} + \text{Action decision} \Rightarrow \text{Cooperation}$$

Multi-target Search

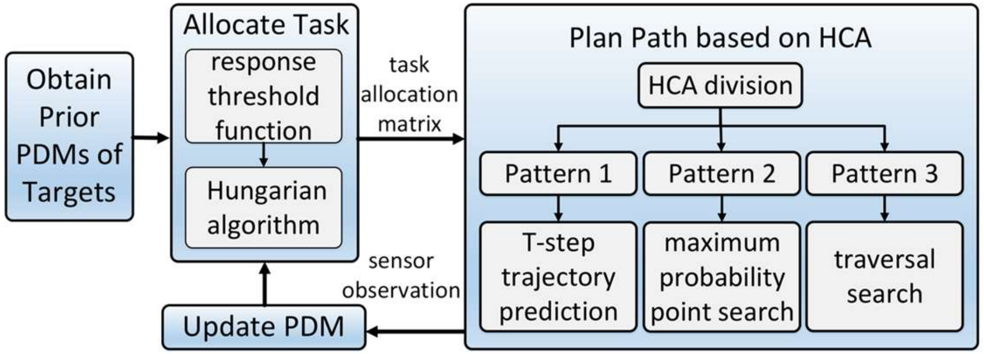
IWIN-FINS

Consider the multi-peak characteristics of probability density map (PDM) for targets search design

Illustration of multi-peak PDM



Algorithm Sketch



HCA-based path planning: **find most probable regions**

- select the most valuable sub-area

$$l^* = \arg\max_{l} \{J^l_{i,j,k}, l = 1, 2, \cdots, g\}$$

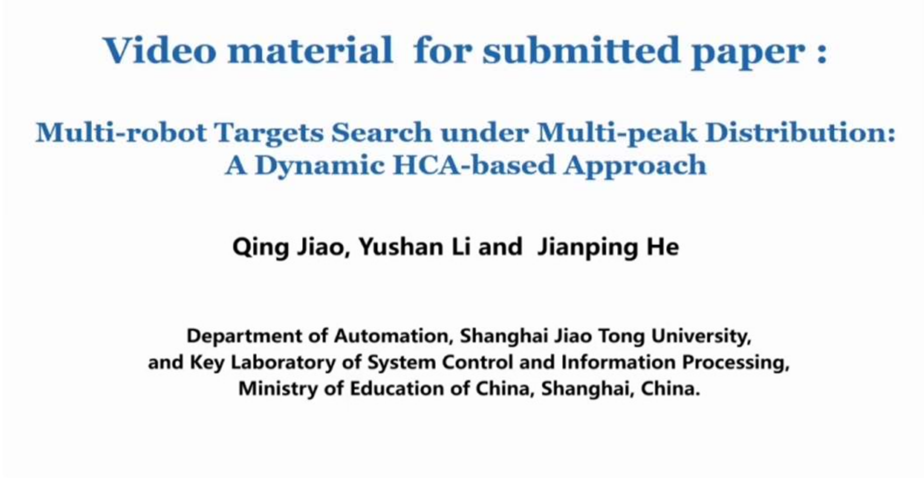
- evaluate HCA

$$J^l_{i,j,k} = \alpha_1 \cdot \bar{f}_{h_j} + \alpha_2 \cdot f_j(w_l^{peak}) + \alpha_3 \cdot |\log\{\beta\|x_{i,k} - w_l^{peak}\|_2\}|$$

- evaluate the path

$$V(x_{\mathrm{i},k}, \pi_{\mathrm{i},k:k+T}) = \sum_{l=1}^{T} \lambda^l \{\mu_1 \cdot P(x_{l,k}, \pi_{l,k:k+T}) + \mu_2 \cdot \|x_{l,k+T} - w^{peak}\|_2\}$$

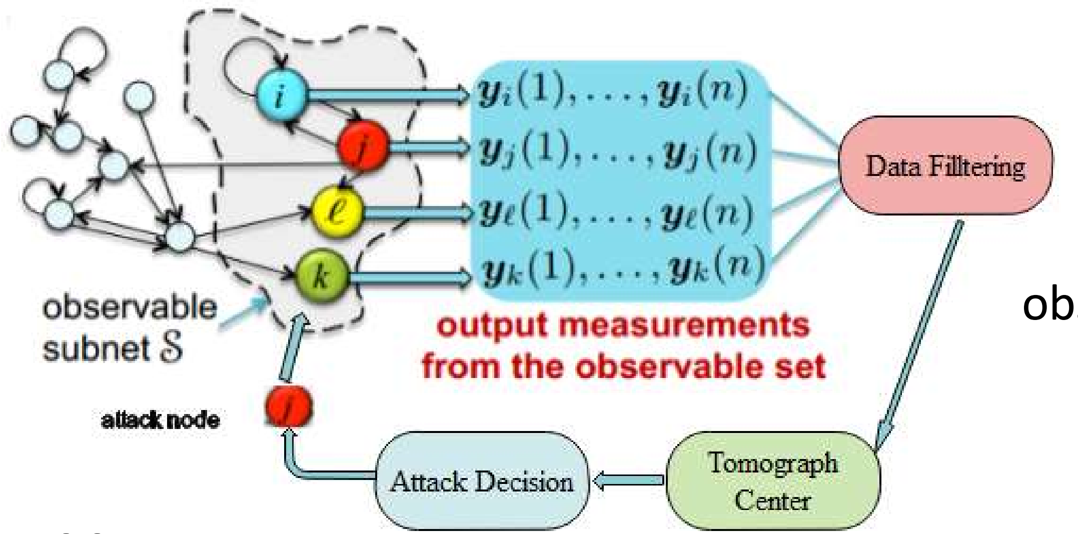
Video Demo



Infer the System Rule

Learning via external observation, and then attack the system

nodes



observer and attacker

Basic problems

- what to observe, how to observe?
- what to learn, how to learn?
- what to attack, how to attack?

① Topology Inference: find the communication topology and attack

② Motion rule learning: find the rule of obstacle avoidance and attack

Acknowledge the primary work of Cong Liu

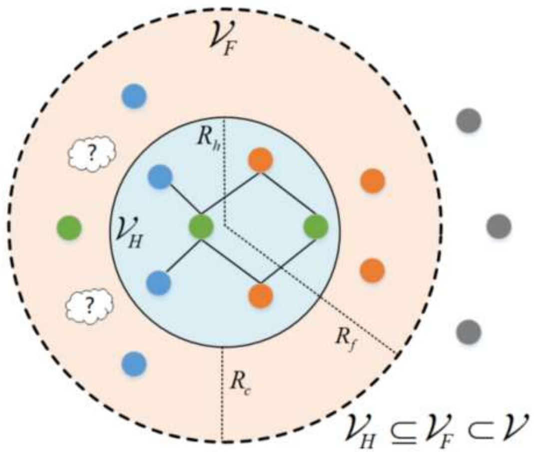
- **C. Liu**, J. He, et al, "Dynamic Topology Inference via External Observation for Multi-Robot Formation Control", 2019 IEEE PACRIM

Topology Inference with Partial Observation

IWIN-FINS

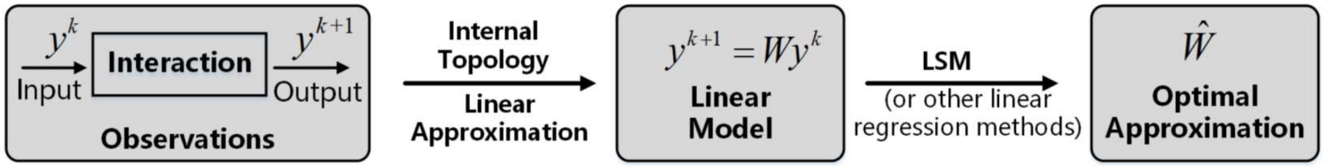
内部拓扑结构决定了系统状态协同的收敛速度和稳定

- 利用稳态数据估计稳定时的状态变化率和偏差
- 基于状态可分离性过滤输入引起的状态变化量
- 针对系统**局部可观**情形，设计了**推断范围收缩**策略



推断范围收缩示意

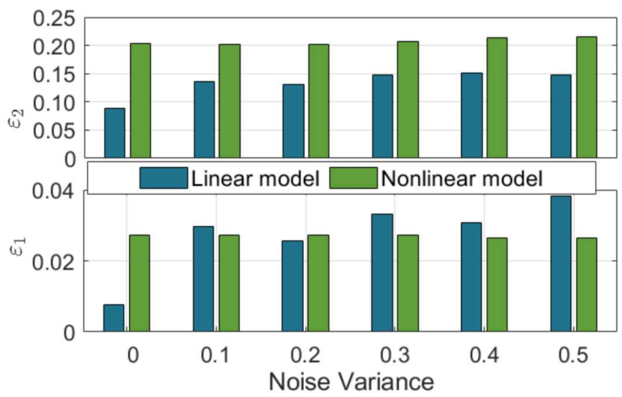
算法原理图



状态的可分离性 $\lim\limits_{t\to\infty} \|z(t) - ct\cdot\mathbf{1} - s\|_2 = 0$

推断范围收缩 $\boldsymbol{E}(y_H^{k+1}) = W_{HF}\boldsymbol{E}(y_F^k)$

均方误差最小化 $\hat{W}_{HF} = \left((Y_F Y_F^\top)^{-1} Y_F Y_H^\top\right)^\top$



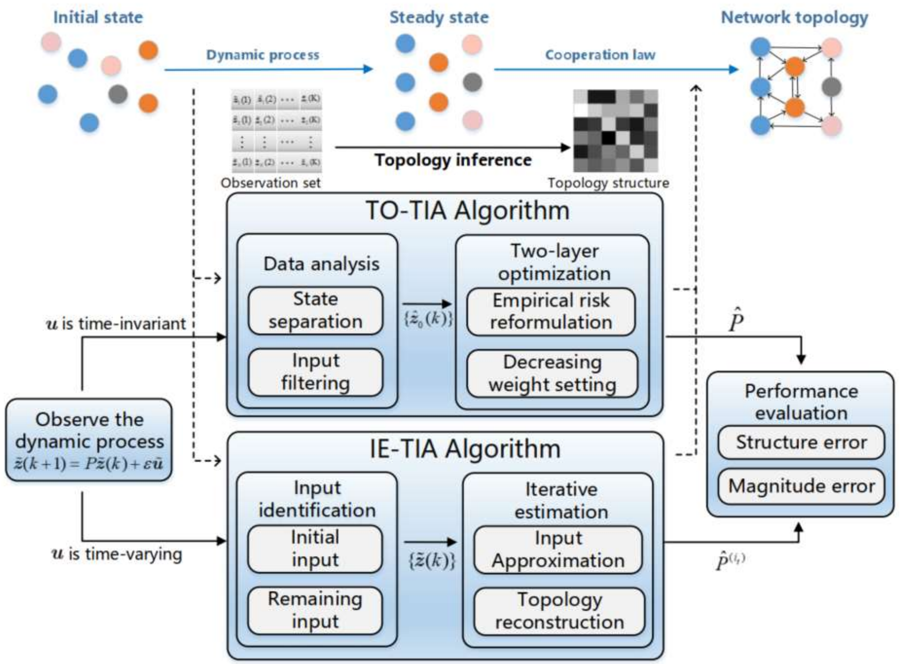
ε_1：结构误差

ε_2：幅值误差

对于不同拓扑动态模型
基于线性推断的方法仍能保证
比较好的拓扑结构推断

Topology Inference with Dynamic Inputs

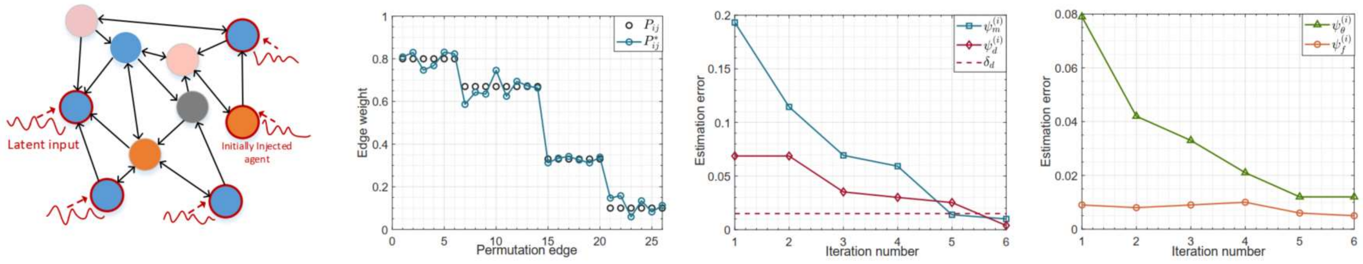
通过滤除输入影响转化为Consensus网络拓扑的推理



- **TO-TIA:**
  the latent input is time-invariant and has already stimulated the network at the beginning of the observation.
- **IE-TIA:**
  the latent input is time-varying and has not stimulated the network at the beginning of the observation.

▶ **Remark**
TO-TIA is not a special case of IE-TIA, and provides direction for IE-TIA on how to identify the latent input and improve the inference accuracy.

- 给出输入可辨识的充分条件
- 设计算法误差渐进有界收敛



(a) (b) (c) (d)

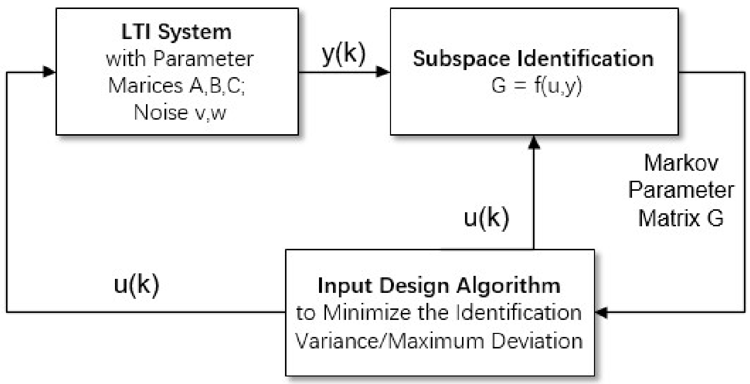
Figure: (a) A visual representation of the network. (b) Off-diagonal entries of P and $\hat{P}^{(i_t)}$. (c) Estimation error of P during the iteration. (d) Estimation error of $\tilde{\mathbf{u}}(k)$ during the iteration.

System Inference with Input design

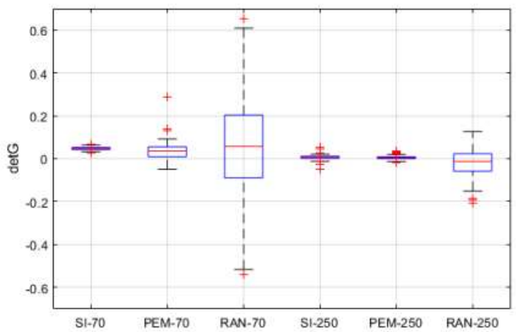
机理推测方法与控制输入设计决定了推断攻击性能

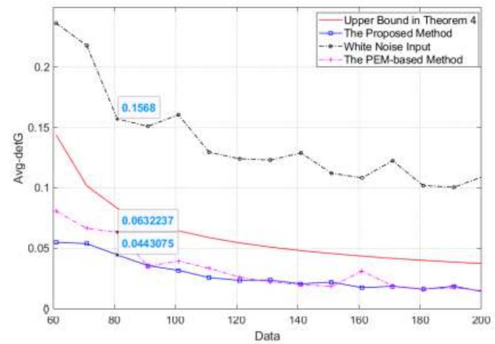
- 提出方法：系统结构子空间系统辨识法、最小方差辨识控制量设计法
- 主要结果：精确辨识的充要条件、系统机理推测结果的性能边界

系统机理实时辨识与控制量迭代优化过程



基于子空间法的最小方差辨识输入





$$\hat{G}(h) = f(u,y) = \frac{1}{N}\sum_{i=0}^{N} Y^c(d:d+s)\mathcal{L}^{-1}[y(k),u(k)]\begin{bmatrix}0\\I_r\end{bmatrix}$$

$$\left\|\hat{G}(h)-G^*(h)\right\|_F^2 \leqslant \frac{c_1}{N}(c_2+t).$$

输入设计可最小化机理防御噪声影响，
最优化子空间法推断性能

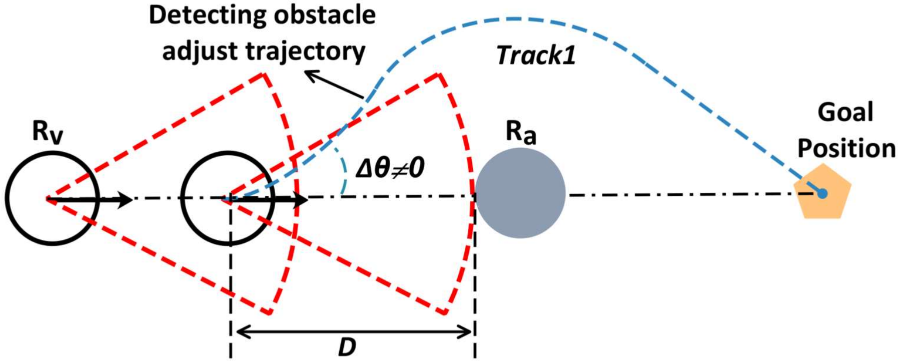
从最优系统激励信号的角度优化推断性能
给出了最优攻击性能下的控制量设计准则

Obstacle-disguising Attack

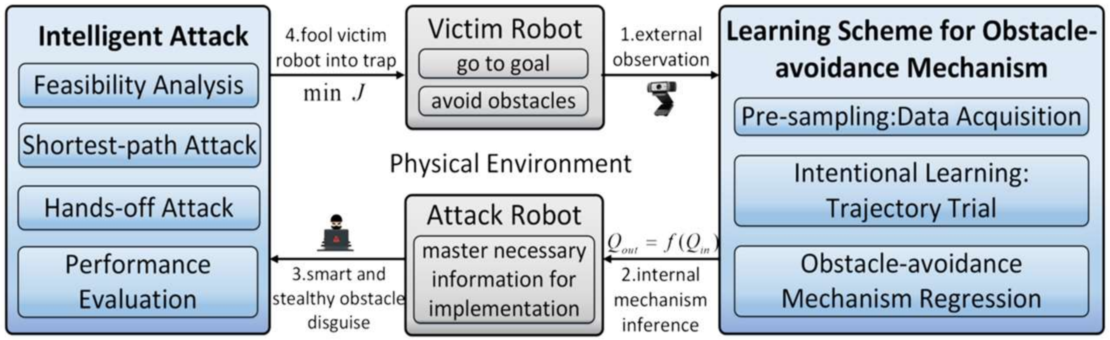
外部交互机制引导机器人避开环境中的障碍物/碰撞

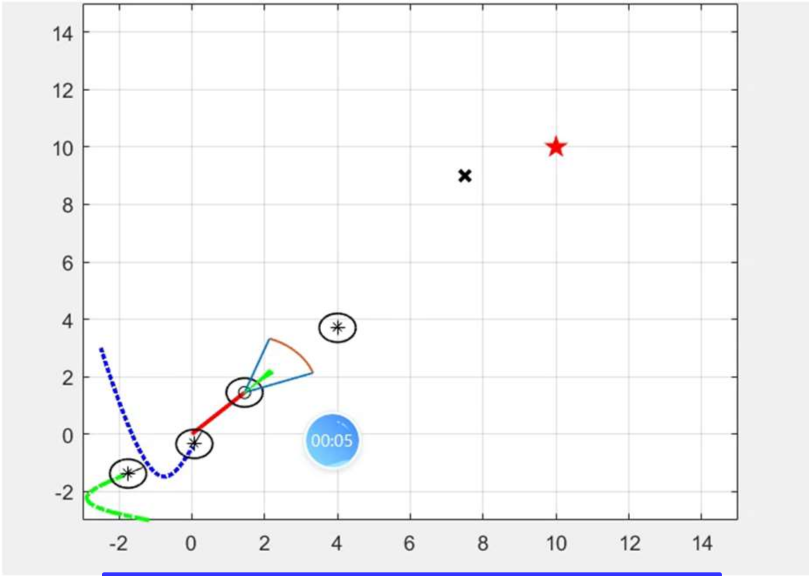
- 设计激励试探的避障机制学习算法
- 设计智能陷阱攻击并给出充分条件
- 给出了**最短路**与**最短时**攻击性能边界

避障学习示意



攻击算法框架





队形生成 状态轨迹　　攻击领航者 诱导至陷阱

最短路攻击

$$\min_{H,\boldsymbol{u}_{a,0:H}} \; C_s(\boldsymbol{u}_{a,0:H}) = \sum_{t=0}^{H} \|\hat{p}_v(t+1) - p_v(t)\|_2,$$
$$\text{s.t. } \|u_a(t)\|_2 \le \sigma,$$
$$\|p_v(H) - p_{trap}\|_2 \le \delta,$$
$$\eta \le \|p_a(t) - p_v(t)\|_2,$$
$$p_a(t) \in DA(p_v(t)),$$

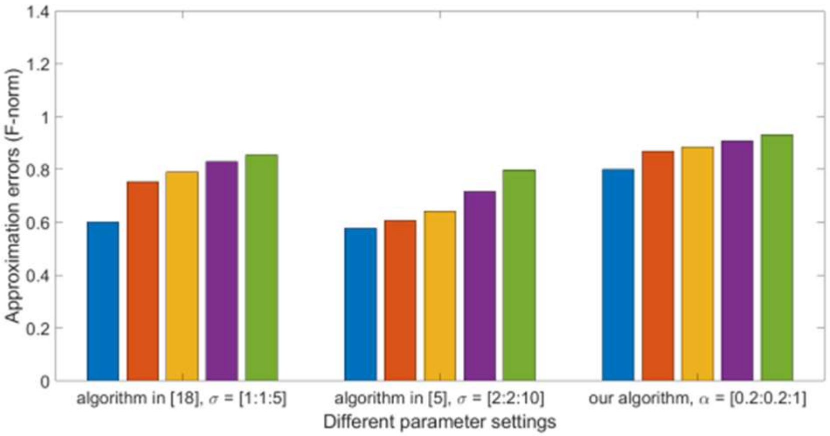
最短时攻击

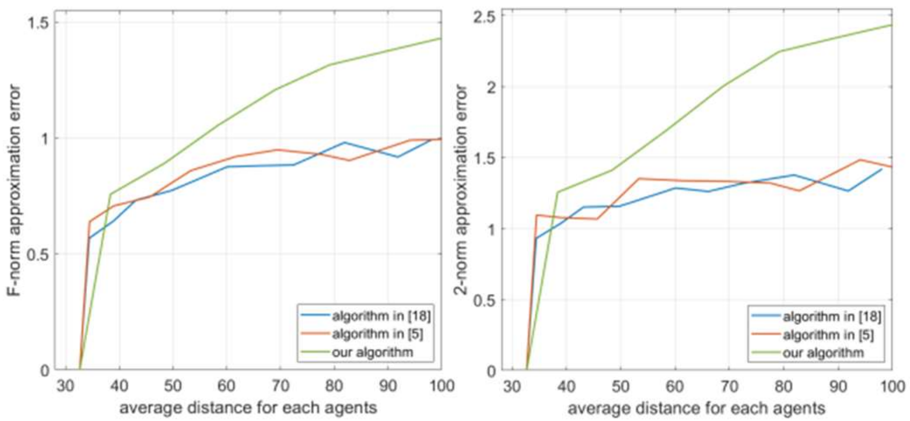
$$\min_{H,\boldsymbol{u}_{a,0:H}} \; C_h(\boldsymbol{u}_{a,0:H}) = \|\boldsymbol{u}_{a,0:H}\|_0$$
$$s.t. \; \|u_a(t)\|_2 \le \sigma,$$
$$\|p_v(H) - p_{trap}\|_2 \le \delta,$$
$$\eta_1 \le \|p_a(t) - p_v(t)\|_2 \le \eta_2,$$

Defense Design for Topology Security

对抗推断攻击的拓扑安全性保护设计

- 任务目标：保护拓扑结构的隐蔽性；保证多智能体系统协同效果
- 提出方法：基于加噪设计的最大化误差问题求解
- 主要结果：基于最小二乘的拓扑推断性能边界、较以往算法更优的安全性和低耗性





设计思路:

- 添加加性噪声 $\theta^+(k)$
- 添加补偿噪声 $\theta^-(k+m) = -W^m \times \theta^+(k)$

$$\theta^+(k) \in \begin{cases} \beta^+(k) = \alpha \times \left(\max\{x_{N_i}(k)\} - x_i^r(k+1)\right), \\ \beta^-(k) = \alpha \times \left(\min\{x_{N_i}(k)\} - x_i^r(k+1)\right). \end{cases}$$

$g_i(X) = \sum_{k=1}^{T} |x_i(k) - x_i(k-1)|$和$\|\widehat{W} - W\|_F$的tradeoff

最优噪声求解 $\max_{\theta(k-1)} \|\Theta(k)Y(k)^{\mathsf{T}}(Y(k)Y(k)^{\mathsf{T}})^{-1}\|_F$

s.t. $\beta^-(k) \le \theta_i(k) \le \beta^+(k)$

收敛速率

$\rho_{ess} = r_{asym}(W) = \max\{|\lambda_2|^2, \cdots, |\lambda_n|^2\}$

Data-Driven Control and Optimization

Distributed optimization plays a vital role in building intelligent networked control systems. We investigate the improvements in both the accuracy and the convergence rates of distributed nonconvex optimization algorithms. To this end, we introduce approximations to substitute for general objective functions as well as constraints, and turn to consider an easier approximate version of the original problem. Furthermore, we pursue dependable distributed optimization in face of various issues ranging from privacy preservation to resilience against malicious adversaries.

- Distributed optimization with gradient-free iterations
- Dependable enhancement considering privacy preservation and resilience
- Applications to intelligent multi-robot systems

Kai Luo, PostDoc

Coverage Detection

Zhiyu He, MS

Non-convex Optimization

Xiaoyu Luo, PhD

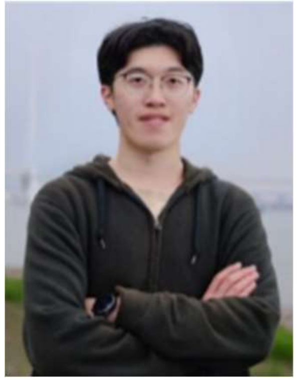
Fault-tolerant Control

Wenzhe Zheng, MS

Attack Compensation

Jialun Li, MS

Unpredictable Control

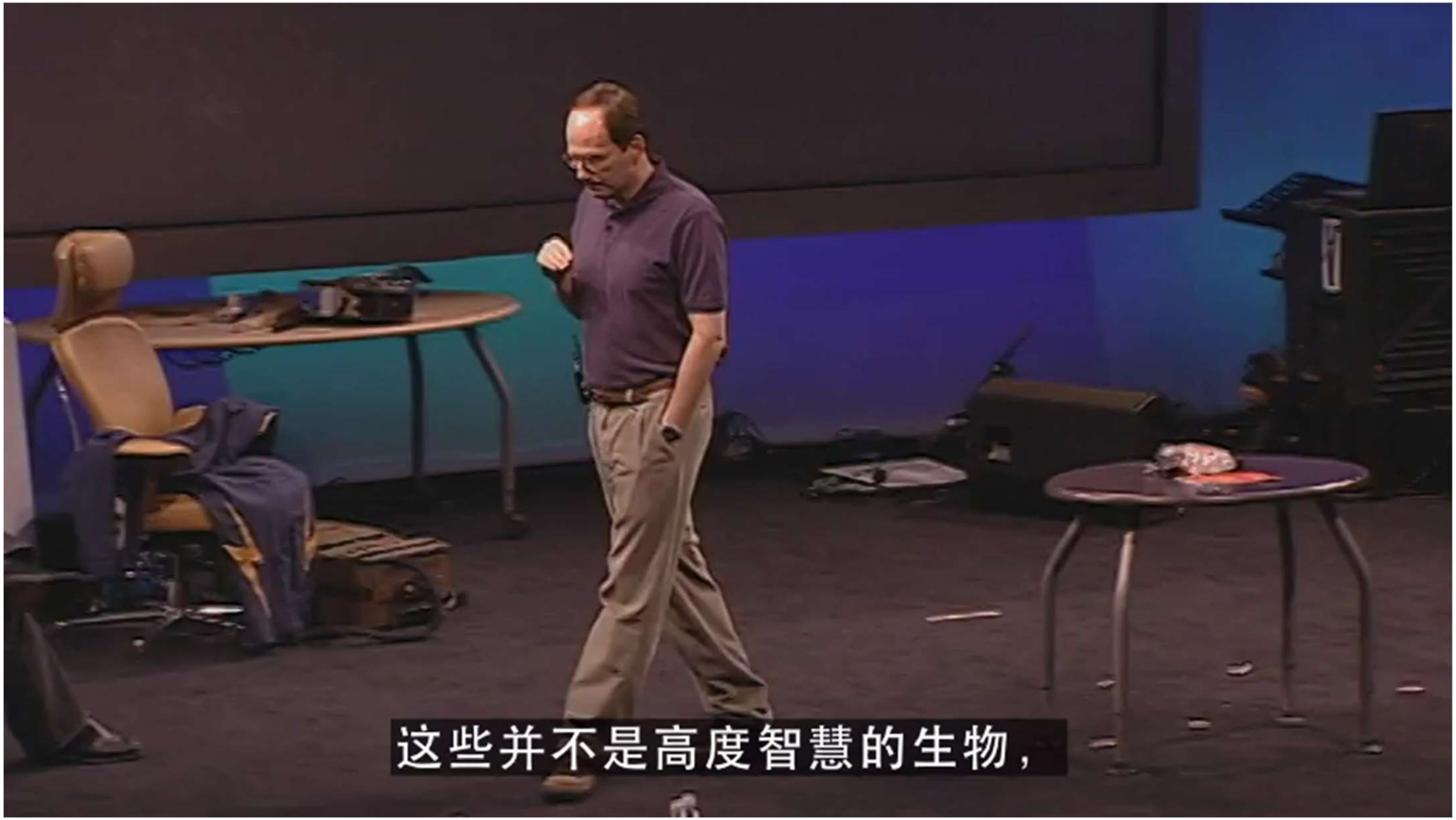


Xuechao Zhang, MS

Learing algorithm

Cooperative Control

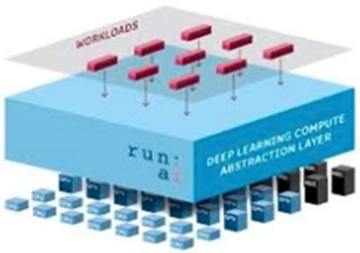
IWIN-FINS



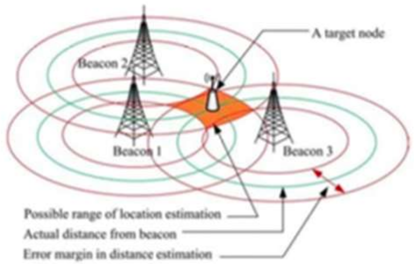
Distributed Optimization

IWIN-FINS

- Distributed optimization arises in many applications related to networked systems.

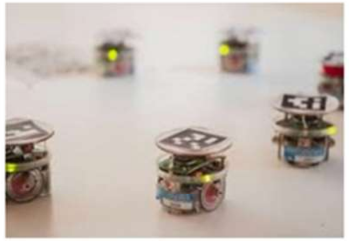


(a) Distributed Machine Learning[1]



(b) Distributed Localization in Sensor Networks[2]

(c) Distributed Coordination in Smart Grids[3]



(d) Distributed Control of Multi-robot Systems[4]

Figure 1 Application scenarios of distributed optimization

---

[1] S. Boyd *et al.*, *Found. Trends Mach. Learn.*, 2011, [2] Y. Zhang *et al.*, *IEEE Trans. Wireless Commun.*, 2015, [3] C. Zhao *et al.*, *IEEE Trans. Smart Grid*, 2016, [4] H. Jaleel *et al.*, *Proc. IEEE*,

Distributed Optimization

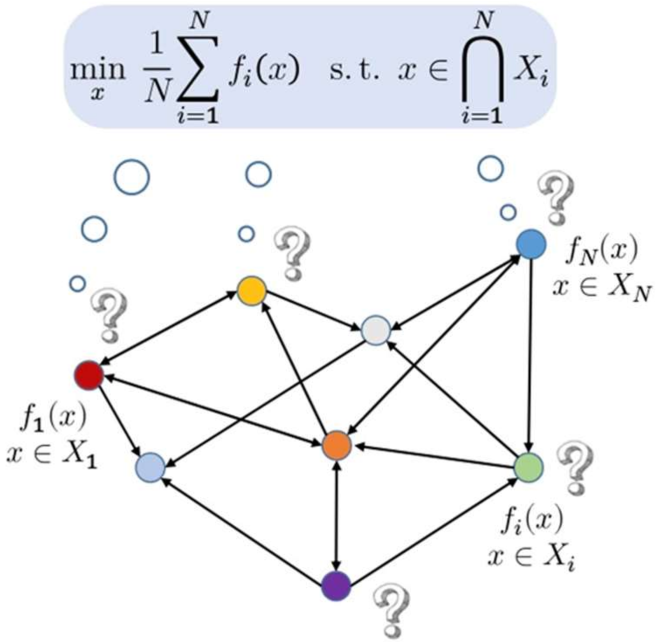


Figure 2 An illustration of distributed optimization

- What is Distributed Optimization (DO)?

Agents optimize a global objective function based on local computations and communication.

- Why not Centralized Optimization (CO)?
  - possible lack of central authority
  - issues of efficiency, robustness & scalability[5]
- Any Critical Challenges?
  - comparable convergence to CO (widely studied)
  - preserve privacy of sensitive local information

[5] A. Nedić *et al.*, "Distributed optimization for control," *Annu. Rev. Control Rob. Auton. Syst.*, 2018

Distributed Optimization

IWIN-FINS

Developments of Distributed Optimization

A. Nedich
ASU

DGD
undirected graph
sub-linear rate
(2009)

W. Shi
Princeton

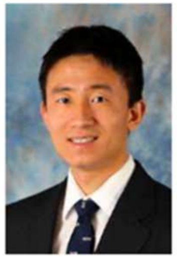
EXTRA
undirected graph
linear rate
(2015)

A. Olshevsky
BU

Push-DIGing
directed graph
linear rate
(2017)

G. Scutari
Purdue

SONATA
directed graph
(2019)
1st-order



M. Hong
UMN

ZONE
undirected graph
(2019)
0th-order

DGD, EXTRA, Push-DIGing: 1st-order convex optimization algorithms

SONATA, ZONE: non-convex optimization algorithms

Motivation

General Distributed Optimization

$$\min_{x\in X} \; f(x) = \frac{1}{N}\sum_{i=1}^{N} f_i(x)$$

↑ possibly noncovex

Generic Methods with Gradient Tracking

$$x_i^{t+1} = \mathcal{F}_t\left(\sum w_{ij}x_j^t, s_i^t\right)$$

$$s_i^{t+1} = \sum w_{ij}s_j^t + \underbrace{\nabla f_i(x_i^{t+1}) - \nabla f_i(x_i^t)}_{\text{eval of gradients at every itr}}$$

Notable unresolved issues in the existing work

- growing load of oracle queries with respect to iterations
  - ▷ results from evaluations of gradients or values of local objectives at every iteration
- hardness of achieving iterative convergence to global optimal points
  - ▷ results from the nonconvex nature of general objectives
- trade-off between privacy and accuracy for differentially private DO algorithms

Algorithm Overview

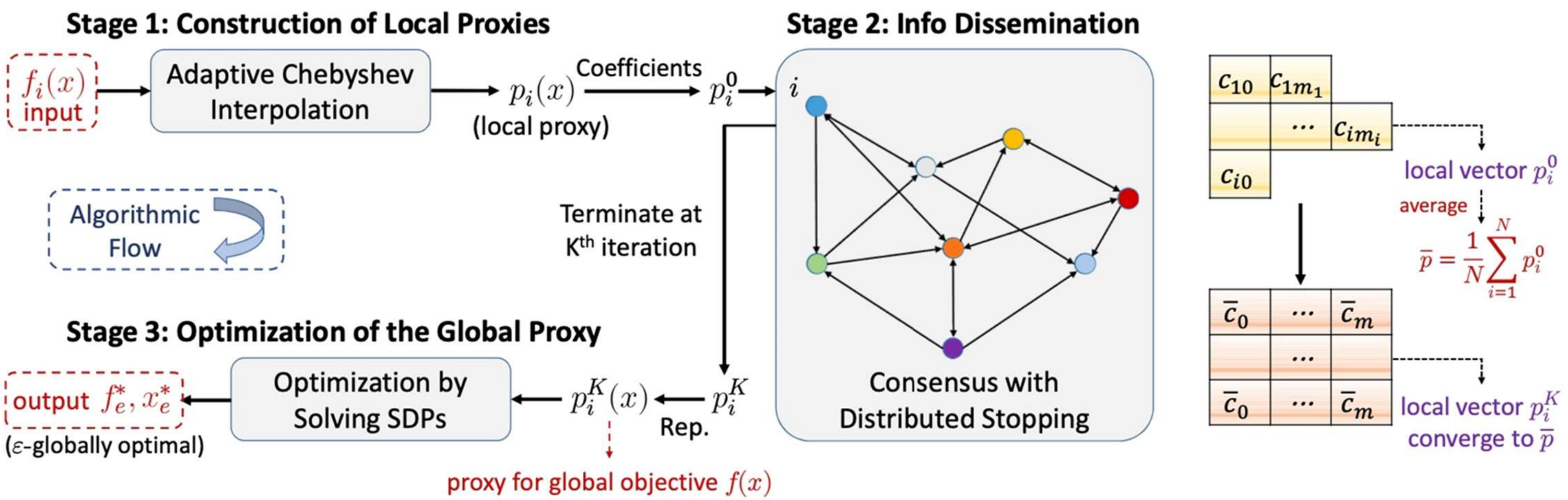


Figure 3 The architecture of D-CPOA

Distributed Learning and Optimization

IWIN-FINS

北京大学 Peking University

Time: July 7th, Tuesday, 14: 30 - 16: 30
Zoom link: ethz.zoom.us/j/5258434015
Zoom meeting ID：525 843 4015

智能控制系列报告

报告人: 何志宇 (上海交通大学博士生)
报告题目：Non-convex Distributed Optimization: Novel Algorithmic Design and Arbitrarily Precise Solution

报告人: Jeremy Coulson (苏黎世联邦理工学院博士生)
报告题目：Regularized & Distributionally Robust Data-enabled Predictive Control

主持人: 梅文俊 (苏黎世联邦理工学院博士后)
主办单位：北京大学智能控制实验室

北京大学 Peking University

Zoom会议链接：ethz.zoom.us/j/5258434015
时 间：7月7日, 星期二, 14: 30 – 15: 30
会 议　ID：525 843 4015

智能控制系列报告

Non-convex Distributed Optimization: Novel Algorithmic Design and Arbitrarily Precise Solution

Abstract: This talk will introduce a novel distributed algorithm (named CPCA) by exploiting Chebyshev polynomial approximation, consensus and SDP theories, to solve a class of constrained distributed non-convex optimization problem. Different from existing iterative gradient-based method, this algorithm has the advantages of being i) computationally efficient in that no evaluation of gradients is required within the iterations, and ii) able to obtain arbitrarily precise estimates of global optimal solutions. We prove that with O(m) zeroth-order oracle queries and O(log(m/epsilon)) rounds of communications, CPCA can yield epsilon globally optimal solutions for the considered problem, where epsilon is any arbitrarily small given tolerance, and m is the maximum degree of local approximations. Extensive simulation results validate the effectiveness of the proposed algorithm.

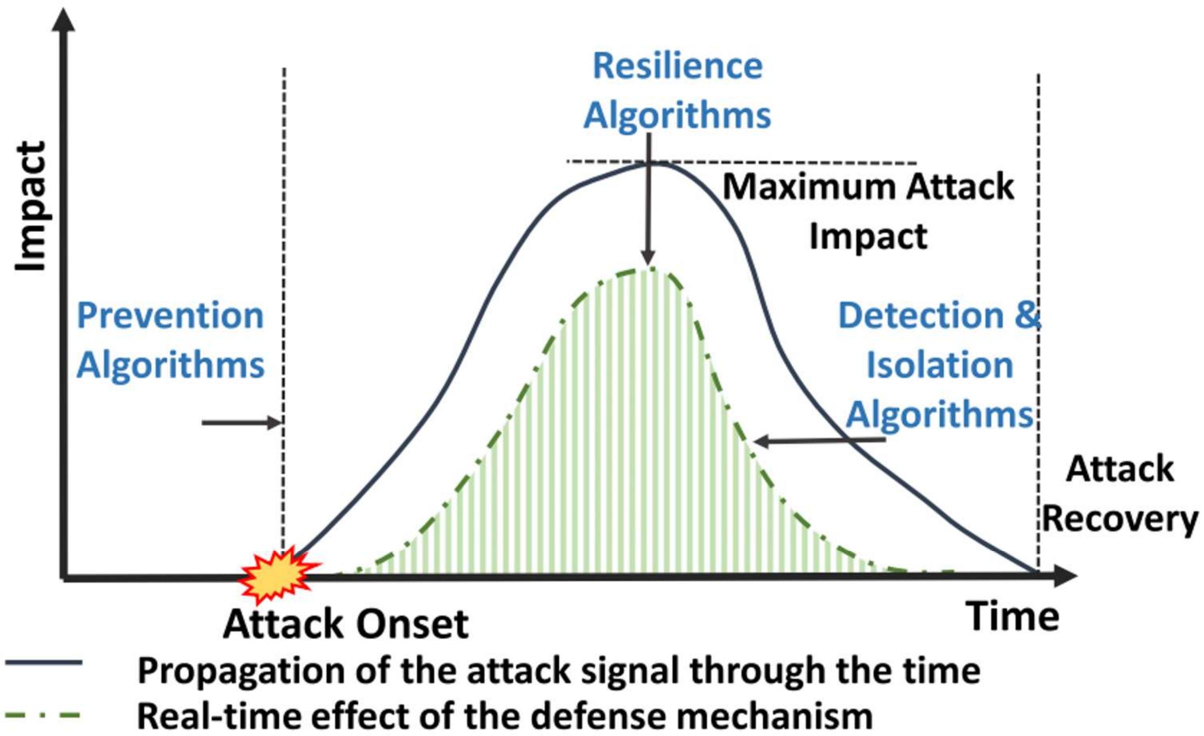
Speaker: 何志宇（上海交通大学博士生）

Biography: Zhiyu He received his B.S. degree in Automation from Shanghai Jiao Tong University, Shanghai, China in 2019, and is currently a master student in the Department of Automation, Shanghai Jiao Tong University, supervised by Prof. Xinping Guan and Prof. Jianping He. His research interests lie in distributed optimization, learning and control of network systems.

主持人：梅文俊（苏黎世联邦理工学院博士后）
主办单位：北京大学工学院智能控制实验室

Secure Cooperative Control

Defense Mechanisms for Resilient Cooperation



- **Prevention**
  Postpone the onset of attacks
- **Resilience**
  constrain the maximum impact of attacks
- **Detection & Isolation**
  infer sensitive info of parameters

防患未然 → 力挽狂澜 → 亡羊补牢

1. Dibaji S M et al., A systems and control perspective of CPS security[J]. Annual Reviews in Control, 2019.

Secure High-dimension Consensus

- **Motivation**

  - Coupled states in different dimensions

    e.g., by complex local dynamics
  - The comparison is difficult

    e.g., sorting and disregarding
  - Enlarge the algebraic connectivity

    e.g., multi-hop broadcasting

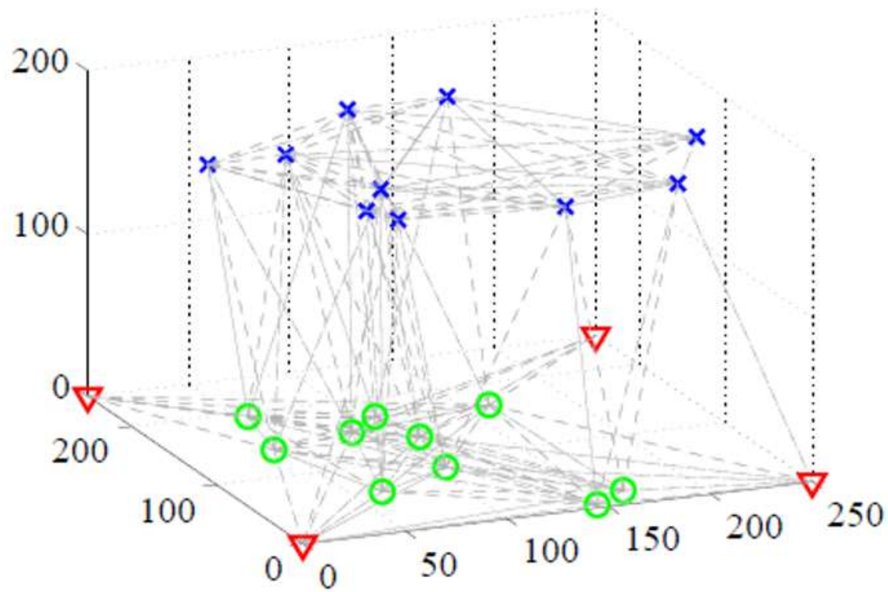
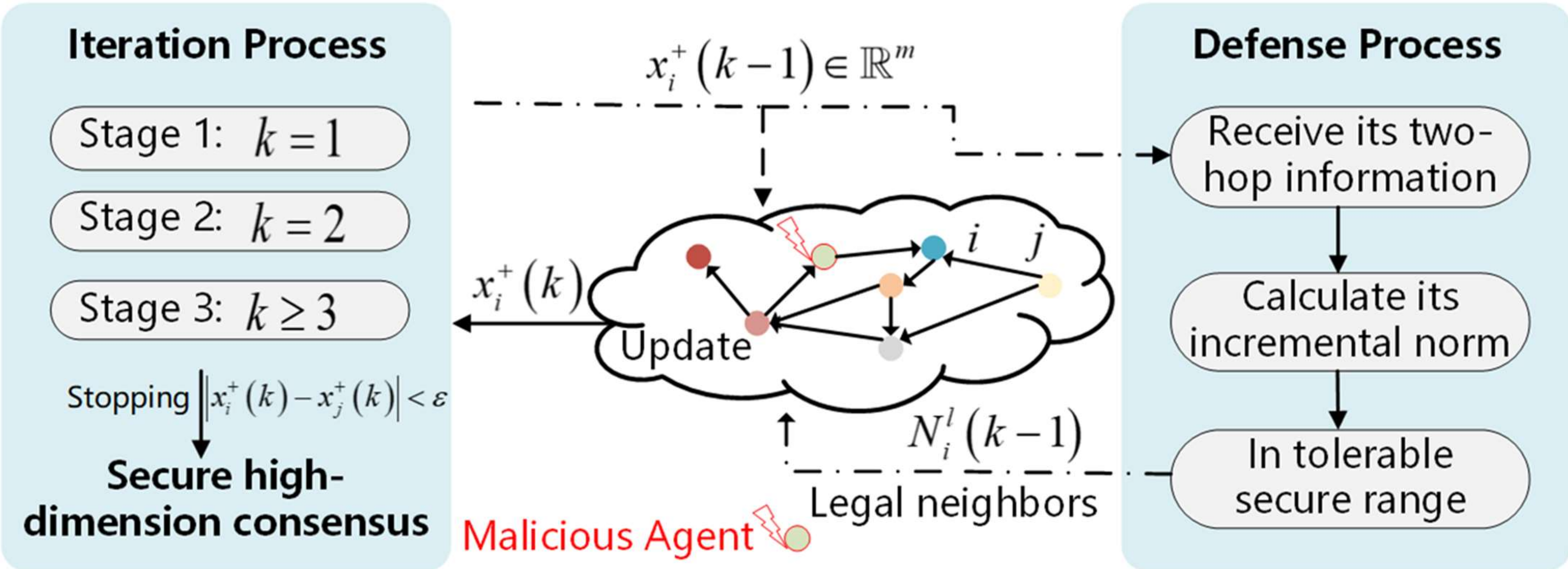


Figure. Symbols: ground robots 'o', aerial robots 'x', and humans '∇'

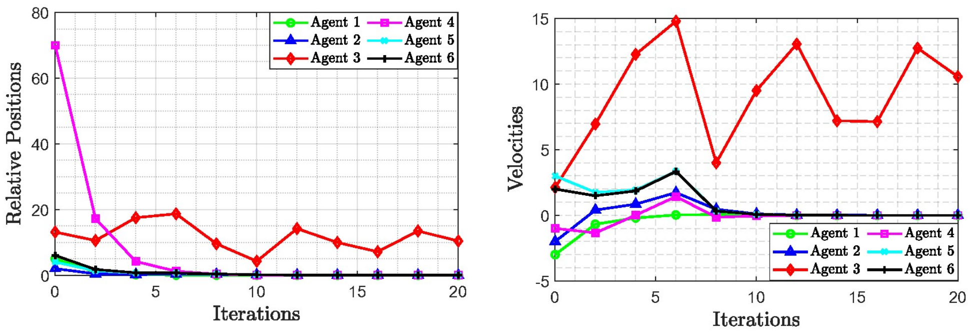
These existing works are not applicable to high-dimension consensus, whose states are coupled

Secure High-dimension Consensus

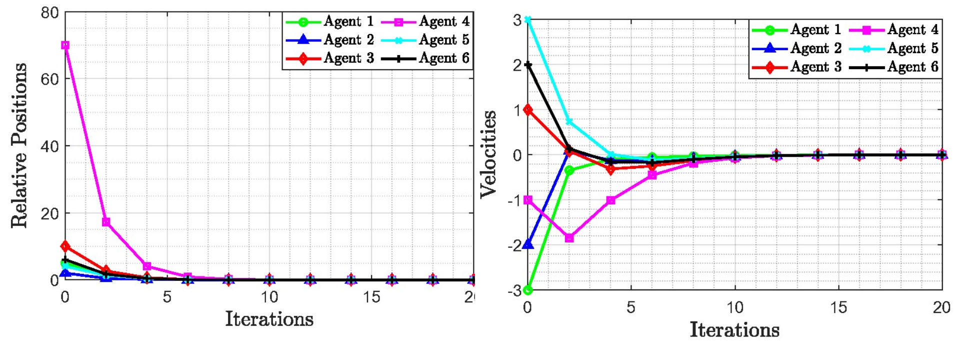
Overview of the SHCA Algorithm design



With the adversary



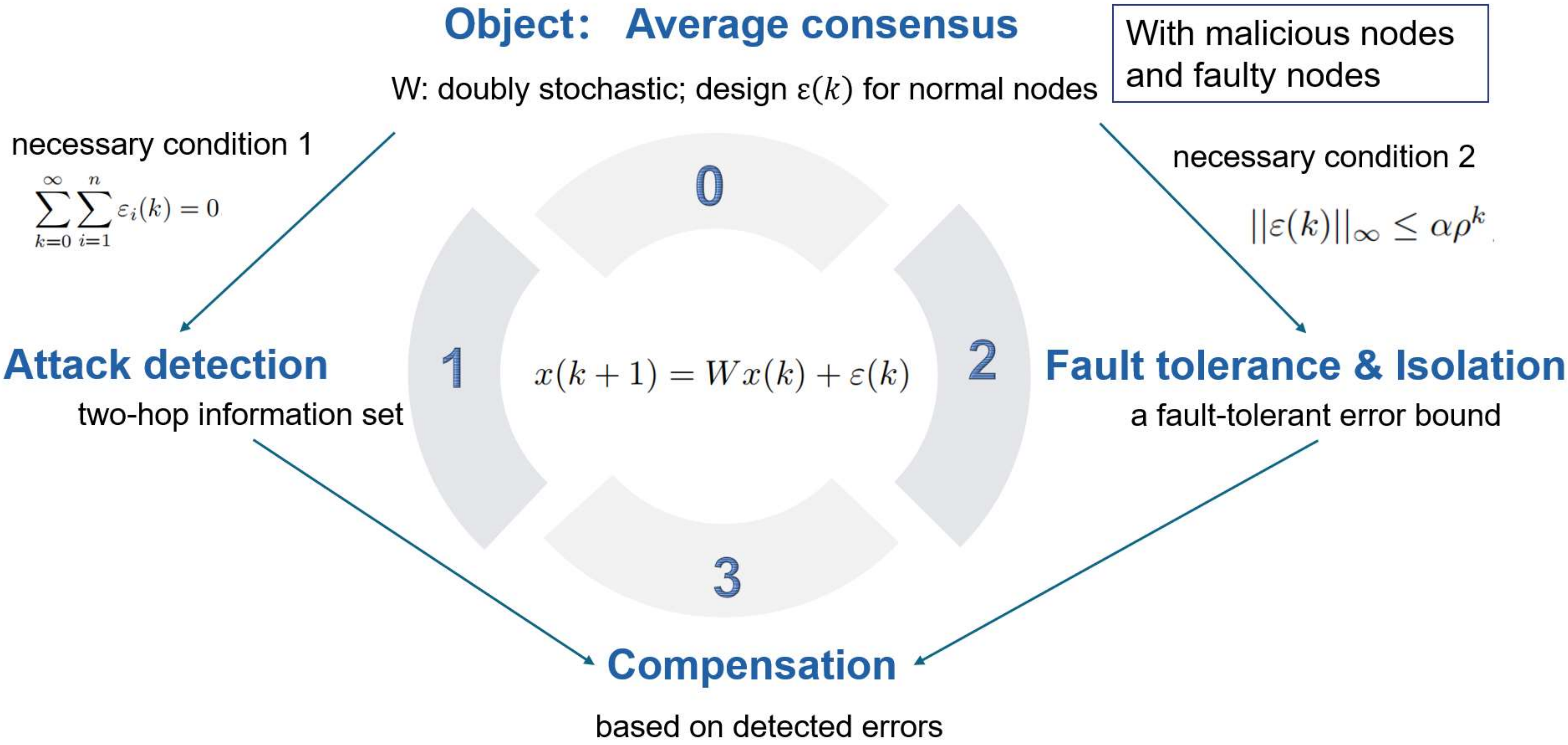
Without the adversary



Resilient Consensus via Detection-Compensation

IWIN-FINS

Overview of the detection and compensation design

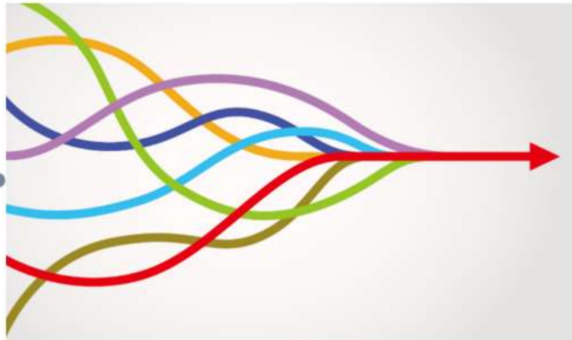


Resilient Consensus via Detection-Compensation

Error Bound: $\alpha_j \rho_j^k$

convergent to zero

out of the error bound: isolation



Compensation Scheme

Scheme 1: impact detected by Detection Strategy I

$$\eta_j^{i(1)}(k+1) = -w_{ij}(x_j^{(i)}(k) - x_j(k))$$

Scheme 2: impact detected by Detection Strategy II

$$\eta_j^{i(2)}(k+1) = -\varepsilon_i^{(2)}(k)/|\mathcal{N}_i|$$

Scheme 3: impact of isolation

$$\eta_j^{i(3)}(k+1) = (x_i(k+1) - x_i(0))/|\mathcal{N}_i|$$

Scheme 4: impact of undetected misbehaviors

$$\eta_j^{i(4)}(k) = -(k-m)\bar{\varepsilon}_i^j$$

{Deterministic, Stochastic} Detection and Compensation Consensus Algorithm {D-DCC, S-DCC} when information sets are available {constantly, intermittently}.

Glimpse of Daily Life

IWIN-FINS

About Research Training

IWIN-FINS

What's Our Training Goal ?

- Establish solid theoretical and technical/hardware foundation
- Develop independent research ability
- Improve academic writing and presentation quality

What Do You Need To Do ?

- Select solid your interested direction
- Focus on your research and balance class work
- Devote time on both theory and platform
- Collaborate closely with seniors/peers
- Report your progress timely

What Will You Acquire

IWIN-FINS

- Chances to talk with distinguished domestic and abroad researchers
- Publish your 1st-author paper on top conferences and journals
- Attend academic conference abroad with fully funded
- Exchange Opportunities to well-known abroad universities

How To Join Us?

IWIN-FINS

- Email to Prof. He (jphe@sjtu.edu.cn) or Dr. Li (yushan_li@sjtu.edu.cn) with your CV, transcript and research experience (not necessary)
- We will appoint an online meeting with you via e-mail

PRP, Chuntsung Projects, Undergraduate thesis are welcomed to apply !

Contact US!

Q&A

Thank You！