WASP Software Engineering & Cloud Computing

Zhaozhan Yao, Dept. Mathematics, KTH
zhaozhan@kth.se

1 Introduction

My research field is control theory. As a branch of applied mathematics, it is a theory to deal with the control of dynamical systems.

My research interest is the synergy of multi-agent systems. The synergy emerges from interactions among individual agents, leading to the formation of groups. Depending on the scale of multi-agent systems (i.e., the number of agents) and available information, two types of problems are considered in my doctoral project: microscopic and macroscopic control.

In the former, the control objective is to achieve some formation in a self-organized way. A particular purpose is that the resulting formation emerges from local interactions among the agents, rather than being fixed or prescribed in advance. Let me draw on an natural example to explain this purpose more clearly. It has been observed in nature that fish swarm form a tightly packed spherical formation, the so-called bait ball, as a defense when sensing the approach of predators. The predators are overwhelmed by the numbers. Such strategy enhances the survival chances of individual fish within the group. It seems that the only purpose is to form a sphere-like formation; the starlings do not care about its size or the exact distances between individuals. This is the point: the exact final formation is unknown and is the result of emergence.

In the latter, the control objective is given in some statistical sense. Due to the huge number of the agents (such as human crowd and starling murmuration), precisely controlling the state of each agent is not necessary; the problem is elevated from the microscopic to the macroscopic level, and the focus now is on controlling the distribution of the overall system state. Modeling and controlling large-scale systems at a macroscopic level is of significant interest to me and is currently in progress.

Finally, I have to acknowledge that I was struggling with this assignment. Since my research project is mainly involved with control theory (mathematics) and I have no experience in AI/ML, I found it difficult to relate those "practical" system engineering arguments and issues to my research.I tried my best to contribute my ideas.

2 Lecture Arguments

2.1 verification and validation

This is one of the arguments that I strongly resonate with, especially its illustrative interpretation: *get the production right* and *get the right production*. In the field of control theory, theoretical rigor and mathematical proof is highly valued and required — get the production right. Typically, we abstract tractable mathematical problems from real-world natural or engineering problems, where simplifying assumptions are introduced (These abstractions and simplifications make the theoretical outcome sound but impose significant practical limitations — this is another story, though.). And this is my point of view: as a researcher in this field, the conducted research should be rooted in real-world problems — get the right production. However, such an approach is somewhat risky in terms of outcome, as it may yield no mathematically provable results. As a result, many papers tend to focus solely on obtaining seem-correct-but-hard-to-follow mathematical proofs, while neglecting whether the system/subject they study are truly grounded in real-world problems.

2.2 science vs. engineering

Control theory, nowadays, is to some extent as esoteric to engineers as building castles in the air. From my point of view, merely addressing the question "why does this work?" is not enough for a competent control theorist; the key lies in conveying the answer in a clear and accessible manner that engineers can also understand. Everyone benefits when the insights gained from studying those "simplified" problems help engineers better understand crucial components in their complex large-scale systems.

3 Guest-Lecture Arguments

3.1 to understand the problem

In my view, the research taste and caliber of a control theory researcher is reflected in his selection of a real-world problem, the abstraction of it into a simplified (mathematical) problem, and the careful balancing of the gap between the two. Chasing seem-correct-but-hard-to-follow mathematical outcome, all the while ignoring the widening gap between the two, is a sign of not 'understanding' the problem, in a control-theoretic perspective.

3.2 solution-space

The idea that I want to express is that a real-world problem can be approached from different perspectives, and in control theory, this leads to the use of different analytical tools and vastly different levels of analytical difficulty. Take crowd evacuation as an example. From a microscopic perspective, we need to deal with each individual. This is not highly recommended, since the focus is on evacuation in a collective sense rather than the precise position or motion of each individual. It is more promising to elevate the problem to a macroscopic level.

4 Data Scientists vs. Software Engineers

- Do you agree on the essential differences between data scientists and software engineers put forward in these chapters? Why or why not?

  Having no experience or expertise in either machine learning or system engineering, I am inclined to agree with the arguments made in the book. Machine learning is still a quickly evolving field. The curriculum for data scientists tends to focus on how machine learning algorithms work or on applying them to develop models for small and clearly defined tasks. This cultivates a model-centric mindset. By contrast, systems engineering is a mature field with both well-established theoretical framework and extensive industrial practice. Software engineers must address less well-defined user requirements, along with constraints such as budget and development timelines — greater uncertainty. This cultivates a system-level mindset and a greater willingness to embrace machine learning, unlike many data scientists resisting system engineering tasks such as deployment, development, and maintenance.

- Do you think these roles will evolve and specialise further or that "both sides" will need to learn many of the skills of "the other side" and that the roles somehow will merge? Explain your reasoning.

  I think both sides need to learn each other's skills, but the roles are unlikely to merge. The first point is simply that the ability to understand and communicate effectively with others is beneficial for everyone in an interdisciplinary team. The second point is that machine learning

is still a quickly evolving field and has not yet reached its foundational depths, as most would agree, and no one knows where it will head in the future. Therefore, I believe that for at least the next decade, the main focus of data scientists will still remain on learning and applying state-of-the-art machine learning algorithms from academia and industry.

5 Paper Analysis: Paper A

The selected paper is entitled "Modeling Resilience of Collaborative AI Systems" from CAIN 2024.

1. **Core idea:** to model resilience of collaborative AI systems (CAIS) when disruptive events occur. To this end, the paper proposes a novel framework, which defines a set of system performance measurements and rules to assess resilience over time. A real-world experiment demonstrates the framework's ability to model CAIS resilience across different performance states (steady, disrupted, and recovered). **Importance:** CAIS performs a task in collaboration with human. It can use a trained AI model or learn online from human interaction based on some sensors. Sensor disruptions can degrade the overall performance, highlighting the need for automated performance tracking to assess the resilience of CAIS.

2. **Relation:** For microscopic control of multi-agent systems, precise control of each agent matters for the collective goal, and thus the idea of resilience is highly important. In some real-world scenarios, the control of each agent relies on interactions with other agents. If interaction of an agent is disrupted, its control strategy might fail, and then the collective goal could be affected.

3. **Integration:** Resilience is also important for multi-agent reinforcement learning (MARL). Typically, MARL studies how a group of agents in a shared environment can learn their own best policy to optimize a global objective. An illustrative example is that a warehouse where multiple robots collaborate to transport items or restock shelves. Using MARL, each robot learns an optimal policy so that the overall system achieves high efficiency in completing warehouse operations. However, some robots may become a source of failures or disruptions due to power outages, system crashes, or even cyber-attacks, which can significantly reduce, or even halt, warehouse efficiency. This motivates the need to consider resilience and that not all agents can be assumed to cooperate — some may be stubborn or even adversarial.

4. **Adaptation:** The idea of resilience can be integrated into multi-agent systems at a microscopic level. Take the previous warehouse system as an example. Since it happens in real world that agents may fail, act unpredictably, or even become malicious, one feasible solution might be to think about reformulating the original MARL as a non-cooperative game between a group of protagonists and antagonists. The former stands for those functional agents while the latter stands for failure or malicious agents. It might be suitable to regard this non-cooperative game as a zero-sum game between two parties while the members within each party are cooperative. Then we can simultaneously train both parties to enhance the resilience of the original MARL. Another adaptation is to consider the so-called open multi-agent systems framework, which is an emerging concept that has gained increasing attention in recent years. Nowadays, drones have been widely used in daily life and even deployed on the battlefield. In terms of resilience, I can come up with an interesting scenario, where a group of drones flying in formation with the purpose of attacking an enemy target. In this process, it is inevitable that some drones will be shot down by the enemy. This turns the system into an open multi-agent system, with agents potentially leaving at any time. As a result, the remaining drones have to alter their formation accordingly. This highlights the necessity of adopting an open multi-agent systems framework when designing control strategies for these drones.

6 Paper Analysis: Paper B

The selected paper is entitled "Engineering Challenges for AI-Supported Computer Vision in Small Uncrewed Aerial Systems" from CAIN 2023.

1. **Core idea:** to investigate the intersection of software engineering and AI, when deploying CV on resource-constrained, edge-based drones. The challenges and solutions related to CV, hardware, software engineering aspects are identified, which provides insights for practitioners developing similar products. **Importance:** There is a substantial body of literature on CV and on software engineering individually, but very little work addresses the software engineering challenges that arise when deploying CV on drones. This emerging area deserves greater attention and research.

2. **Relation:** I think one challenge given in the paper — how to achieve reliable CV in dynamic, uncertain, and resource-constrained environments— resonates with my research in terms of stability and robustness. As mentioned in the paper, many problems in the video stream quality can lead to degrade performance: the environmental uncertainties (e.g., lighting, weather, motion blur) and perceptual noise (e.g., image quality, vibration).

3. **Integration:** Consider that a team of drones is deployed over a disaster zone to locate survivors. Each drone runs an onboard AI model for human detection. The system's AI is not just perception but also collective intelligence: e.g., dynamically coordinating search formations and sharing detection information. Many ideas in the paper such as power management and the use of lightweight CV model can be applied. In terms of software engineering, the paper proposes that the CV pipeline, the hardware component, and the software (that controls the drone and integrates the CV) should be developed and tested individually and then systematically integrated. On the other hand, my research on self-organized formation could dictate how sub-groups of drones fly to maintain communication and optimal perception coverage over an area.

4. **Adaptation:** The adaptations I can make is to introduce various environment/resource constraints into my research problem. Many challenges in terms of measurements can arise due to the dynamic environments for multi-drone systems and their formation control. It is known that global positioning methods like GPS are not suitable for drones, as their accuracy is insufficient, and thus relatively high-precision relative positioning sensors are used. However, measurement errors are still inevitable and must be taken into account in controller design and validation. In terms of communication constraints, assuming a sufficiently intelligent multi-drone system, the communication topology of the entire system is also dynamic due to factors such as line-of-sight occlusion or signal interference. Thus, it is also highly practical to take this factor into account.

7 Research Ethics and Synthesis Reflection

Since my research field is quite distant from software engineering and AI/ML, I have found relatively few suitable papers from CAIN between 2022 and 2025. Initially, I selected papers whose titles contained terms such as "practices" and "principles", or those titled along the lines of "A case study of . . . " or "A framework for . . . ". However, I realized that these papers typically document the development process of their AI-based systems, highlighting the common challenges encountered and the corresponding solutions. Moreover, the issues discussed are not independent; rather, they are interrelated and tightly coupled. After reading these paper, I still found it difficult to extract core ideas that meaningfully connect to my research.

In the second round of paper selection, I focused on papers involving robots, drones, and other autonomous systems. My reasoning was that, although I am unlikely to directly apply their software engineering ideas to my research, these papers can help me understand the practical challenges encountered during the deployment of autonomous systems, which in turn may motivates adjustments to my research. As a result, papers A and B are among the few that allow me to share my thoughts. While paper A includes a real-world (but small) robot arm experiment, what resonated with me more was its focus on modeling the resilience of AI-based systems, which I was able to relate this resilience idea to MARL and discuss from the perspective of my expertise. Paper B discusses in detail the challenges of deploying AI on drone, motivating me to take into account those practical issues when formulating my (mathematical) problems, so that the obtained results remain relevant to real-world applications.

In terms of ethical considerations, I would like to clarify that the ideas and initial draft of this report are entirely my own. I used LLM for text refinement and subsequently made further edits.