李家营

新加坡科技设计大学博士 · 新加坡管理大学研究科学家
年龄：31 · 个人主页：http://jiaying.li · 微信: lijiaying31
手机：(+86) 1881046**** · 邮箱：lijiaying1989@gmail.com

教育背景

新加坡科技设计大学 (SUTD)，信息系统科技与设计学院，博士 2013.09 – 2018.04

- **研究方向**: 形式化验证，程序分析
- **指导老师**: 孙军副教授
- **毕业论文**: Facilitating Formal Verification with Invariant Learning

美国加州大学戴维斯分校 (UCDavis)，计算机科学学院，访问学者 2017.12 – 2018.03

- **研究方向**: 神经网络验证
- **指导老师**: 苏振东教授

中国科学院 (CAS)，计算技术研究所 (ICT)，硕士（肄业） 2011.09 – 2013.06

- **研究方向**: 计算机存储，操作系统
- **指导老师**: 许鲁研究员，詹剑锋研究员

南开大学，软件学院，工学学士 2007.09 – 2011.06

- **成绩排名**: 3.9/4.0, 1/134
- **指导老师**: 李耀国教授
- **毕业论文**: 具有优先调度机制的多任务操作系统内核

工作经历

新加坡管理大学，信息与计算系统学院，研究科学家 2019.10– 至今

新加坡科技设计大学，信息系统科技与设计学院，研究科学家 2018.05 – 2019.09

新加坡科技设计大学，信息系统科技与设计学院，研究助理 2013.07 – 2013.09

研究经历

神经网络的安全性 (鲁棒性) 研究 2019.06– 至今

近些年来，神经网络在很多问题 (比如图像识别、自然语言处理) 的求解上取得巨大进步，因而被应用到越来越多的领域中，甚至包括一些生命攸关的领域，比如自动驾驶、疾病诊断等。但有学者发现神经网络在安全性上是脆弱的 (比如容易受到对抗样本攻击)。本课题研究如何测试和验证神经网络的安全性。

Socrates: 神经网络分析的统一框架

- 本项目提供一套统一的神经网络分析框架，以方便研究者开发、扩展、测试和评估各种神经网络分析技术。具体来说，Socrates 定义了一套可扩展的格式来统一描述各种类型的神经网络的架构和参数，同时开发了一套新的断言系统来表达待分析的网络性质。该系统核心部分内置了多种神经网络分析引擎的具体代码实现，包括基于假设检验、数值优化、抽象解释和抽象精化等方法的网络分析方法。

DeepRefine: 神经网络验证中可解释的抽象精化技术

- 抽象精化技术可以用来提升基于抽象解释的系统分析精度，但在神经网络验证中抽象精化的方法通常面临着难以解释的问题 (比如什么时候精化、为什么精化)。本项目基于 DeepZ 和 DeepPoly 两种抽象域提出一种可解释的抽象精化方法。具体来说，当当前抽象无法验证所需性质时，我们 1. 使用优化算法去检验网络每层的抽象；2. 通过搜索去找出最早的不合适的抽象；3. 利用梯度信息对该抽象进行精化，从而使得目标性质更有可能得到验证；4. 如果精化后，性质仍无法验证，则重复以上步骤。

AdvSearch: 一种对抗样本生成和检测的统一视角

- 对抗样本的生成和检测是神经网络安全性研究的重点。本项目试图将对抗样本生成和检测问题统一转化成对抗样本搜索问题：在一个样本附近搜索不同标签的样本。一方面，对抗样本生成通常是在一

个正常样本附近搜索不同标签的样本的过程；而另一方面，相比于正常样本，对抗样本在统计上距离神经网络的决策边界更近，因此可以通过在给定样本附近搜索不同标签的样本的难易程度来判断一个样本是正常样本还是对抗样本。更进一步，通过对几种基于优化的搜索算法的建模，本项目提出一种搜索难易程度的度量，从而解释了为什么 (非自适应) 对抗样本检测通常比对抗样本生成更容易。

智能合约的验证和优化技术研究 2018.05 – 2020.10

智能合约是部署在区块链上的程序，它允许非互信双方在没有第三方参与的情况下进行可信交易 (经常涉及资金转移)。合约中通常不可避免地存在代码漏洞，且一旦部署则难以修改，这使得智能合约的正确性、安全性极为重要。本课题研究如何对智能合约进行安全性验证，并基于验证来优化合约的 gas 消耗。

sVerify: 智能合约的 unbounded 验证技术

- 现有智能合约分析工具通常只能对合约做有界 (bounded) 测试或验证，而本项目旨在实现 unbounded 验证。sVerify 首先构建智能合约的控制流程图，然后使用符号执行技术对合约中的路径进行求解。当遇到循环结构时，sVerify 通过调用多种分类算法 (支持向量机 + 决策树) 来自动生成相应的循环不变式，将循环结构的验证转化成无循环程序的验证，从而实现智能合约的 unbounded 验证。

sOptimize: 基于验证的智能合约 gas 优化方法

- 为了实现可信交易，用户在创建、部署和执行智能合约时需要支付一定费用 (gas)。本项目旨在自动优化智能合约的 gas 消耗。具体来说，通过预定义了一些优化规则，sOptimize 对合约代码进行规则匹配来发掘可能的优化机会，然后使用测试和验证的方法从中筛选出安全的优化，从而进行代码移除、修改。经过优化的智能合约，与原始合约在功能上是等价的，且可以直接部署在区块链上。

软件验证中循环不变式的生成技术研究 2015.06 – 2018.12

在计算机程序中，循环 (或递归) 结构一直是各种软件分析的重点 (假如没有循环，很多程序分析问题会变得非常容易且直接)。而循环不变式的发掘也是编译优化、程序分析和软件验证中的一个基础性问题。本课题旨在研究如何利用机器学习算法来自动生成循环不变式，以帮助程序的自动化验证。

Zilu: 基于数据驱动的循环不变式生成技术

- 本项目提出一种基于机器学习算法来生成循环不变式的方法。给定程序和待验证的性质，Zilu 1. 通过对程序状态进行采样，并依据运行时信息对这些状态进行标记从而建立数据集；2. 使用机器学习算法 (支持向量机及其变种) 对数据进行分类，并将分类模型转化成循环不变式候选，然后利用选择性采样的方法对该候选做修正；3 使用 z3 约束求解器来检验该候选是否满足循环不变式的条件 (是否可以验证目标性质)；4. 如果不满足，则生成反例加入数据集，重复上述过程来对该候选做进一步修正。

Zimu: 基于状态划分的复杂不变式生成技术

- 有些循环结构的验证需要复杂的循环不变式（比如含有析取形式的表达式），而自动生成这些不变式相当困难。本项目提出一种通过对程序状态进行动态划分，利用简单的学习算法来生成复杂的循环不变式的技术。具体来说，Zimu 根据循环结构的控制流图对收集到的数据进行划分，使得不同划分对应不同的控制流，而后者对应着不同的“划分不变式”，因而可以对每个划分的不变式分别进行学习。然后把这些生成的划分不变式候选和相应的控制约束组合成循环不变式候选，来完成对循环的验证。

其他研究 2010.10 - 至今

bvSolve: 智能合约中的位向量约束的快速求解方法

- 智能合约的分析通常会涉及 (256 位) 位向量约束的求解，目前的方法 (bit-blasting) 在处理这些约束时不够高效。本项目通过将其转化成语义等价的整数约束，利用整数约束求解技术来提升其求解效率。

iKLEE: 一种基于混合语义的 KLEE 程序分析方法

- 学习算法生成表达式通常是整数语义的，但程序中的表达式却是位向量语义的。本项目基于 KLEE，通过对不同语义进行严格的编解码，使得 KLEE 中位精度的程序分析可以支持整数语义的表达式。

ptaLearn: 基于主动学习的带参时间自动机的验证方法

- 带参时间自动机可以用来建模、分析和验证时变系统，其验证过程需要合成参数必须满足的约束条件。本项目使用主动学习的方法来生成该约束从而可以利用无参模型检测器来验证带参时间自动机。

miniKernel：多任务微内核操作系统的实现

- 本项目是本科毕业设计的课题，旨在学习和实践操作系统的基本功能。该系统建立在 bochs 模拟器上，工作在 x86 保护模式下，实现了包括进程调度、内存、文件和 I/O 管理等操作系统的基本功能。

论文

- Towards Interpretable Abstraction Refinement for Neural Network Verification [投稿中, 2021]
  Jiaying Li
- Improving DeepPoly through Abstraction Refinement [投稿中, 2021]
  Long H. Pham, **Jiaying Li**, Jun Sun
- Verification Assisted Gas Reduction for Smart Contracts [投稿中, 2021]
  Bo Gao, Ling Shi, **Jiaying Li**, Jun Sun
- SOCRATES: Towards a Unified Platform for Neural Network Analysis [投稿中, 2021]
  Long H. Pham, **Jiaying Li**, Jun Sun
- sVerify: Verifying Smart Contracts through Lazy Annotation and Learning [投稿中, 2021]
  Bo Gao, Ling Shi, **Jiaying Li**, Jialiang Chang, Jun Sun and Zijiang Yang
- Deep Clustering by Gaussian Mixture Variational Autoencoders with Graph Embedding
  Linxiao Yang, Ngai-Man Cheung, **Jiaying Li**, Jun Fang
  International Conference in Computer Vision (ICCV'19), Seoul, Korea, 2019
- Learning Loop-invariants with Program Structure-based State Partitioning [预印本, 2018]
  Jiaying Li, Jun Sun
- Classification-based Parameter Synthesis for Parametric Timed Automata
  Jiaying Li, Jun Sun, Bo Gao and Étienne André
  International Conference on Formal Engineering Methods (ICFEM'17), Xi'an, China, 2017.
- Automatic Loop-invariant Generation and Refinement through Selective Sampling
  Jiaying Li, Jun Sun, Li Li, Quang Loc Le and Shang-Wei Lin
  IEEE/ACM International Conference on Automated Software Engineering (ASE'17), Illinois, USA, 2017.
- Scaling BDD-based Timed Verification with Simulation Reduction
  Truong Khanh Nguyen,Tian Huat Tan, Jun Sun, **Jiaying Li**, Yang Liu, Manman Chen, Jin Song Dong
  International Conference on Formal Engineering Methods (ICFEM'16), Tokyo, Japan, 2016.
- An Invariant Inference Framework using Active Learning and SVMs
  Jiaying Li
  International Conference on Engineering of Complex Computer Systems (ICECCS'15), Gold Coast, Australia, 2015.

所获奖励

- 新加坡科技设计大学校长奖学金 2013 - 2018
- 国家助学金 2010 - 2011
- 国家奖学金 2009 - 2010
- 国家励志奖学金 2008 - 2009
- 国家助学金 2007 - 2008

学术服务

- 会议审稿: APSEC 2016, ICECCS 2017, SATE 2018, ICFEM 2018, ICFEM 2019, TASE 2019, FormaliSE 2019，AST 2020, SETTA 2020，IMLSE 2020，Internetware 2020
- 课程助教: 机器学习 (本科, SUTD, 2014)、软件构造原理 (本科, SUTD, 2014)

主要技能

- 工作语言: 中文，英语
- 编程语言: Python, C, C++, Shell
- 精通领域: 形式化验证，神经网络安全性，测试
- 熟悉领域: 软件分析，深度学习，约束求解