

《计算科学导论》课程总结报告

|  |  |
| --- | --- |
| 姓 名 | 茆星远 |
| 学 号 | 2107020318 |
| 专业班级 | 本研人工智能2101 |
| 学 院 | 计算机科学与技术学院 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程认识  30% | 问题思考  30% | 格式规范  20% | IT工具  20% | 总分 | 评阅教师 |
|  |  |  |  |  |  |

2021年12月31日

# 1 引言

计算科学的发展历史并不长，但发展成果却非常丰富。作为计算机类专业的新生，想要完全掌握这些知识难度很大，但对其有一个整体的认识和把握却十分有必要。计算科学导论便是这样一门在使我在学到初步知识，对未来发展能有一定认识的同时，在更高层次上指出了针对一个学科如何认知和如何导学的一整套科学的思想方法的课程。可以说对于我们大一新生来说，这样一门课是必不可少的，结课后，我对这门课以及整个计算科学也有了很深的体会。

# 2 对计算科学导论这门课程的认识、体会

在我看来，计算科学导论这门课程是一门出发点高、引导性强、能极大拓展学生视野的课程，下面将分别论述。

## 一、课程立足哲学，出发点高

课程从科学哲学的思想方法出发，全程贯穿科学哲学和学科方法论。要知道哲学是科学的指路人，一切科学都是哲学的产物，科学是哲学思维延伸到现实领域的逻辑模型体系。课程立足于哲学，让我在学到初步知识的同时，在更高层次上了解到了针对一个学科如何认识的一整套科学的思想方法。

例如课程的第一章中对科学哲学与学科方法论做了简单介绍，从西方哲学的转变讲起，分别介绍了本体论、经典认识论、知识论等内容。这不仅大大丰富了我的知识面，更是转变了我对哲学本身以及对哲学和科学的根本认识。

正如罗素所说的一样，哲学的最高目标就是养成一种批判的意识和怀疑的精神，哲学对任何被视为绝对真理的东西永远高昂着不屈的头颅。与其说哲学是一种具体的学科，不如说哲学是一种坚持用思辨来追问一切、质疑一切的态度。一部哲学史即人类先贤就一切问题的一切思考引起的宏伟辩论。同时，每个时代最激烈的问题又不尽相同，继而称哲学为时代的精华并无不妥。

而自然科学的迅猛发展和关于科学知识真理性问题的讨论，促使科学哲学应运而生。科学哲学是20世纪兴起的一个哲学分支，关注科学的基础、方法和含义，主要研究科学的本性、科学理论的结构、科学解释、科学检验、科学观察与理论的关系、科学理论的选择等。该学科的中心问题是：什么有资格作为科学，科学理论的可靠性，和科学的终极目的。

随着科学哲学而来的，便是一般的科学的思想方法。面对一个待解决的问题，有没有什么更一般的方式方法或工作原则来指导和帮助我们较好地解决这个问题？课程总结了科学哲学的思想方法与处理问题方式方法的三步曲：一个科学的认识、一套科学的方法以及一套科学的程序。这让我在大学生活刚开始时，便从一个很高的层次把握了解决各种问题的方法，可以遇见对我以后的学习生活产生很大益处。

在我没有学习这门课程之前，我从未意识到哲学与科学之间的紧密联系，更不用说哲学与我所学习的计算机专业之间的关系。而课程的内容重在引导我们怎么从科学哲学的角度去认识和学习计算科学，让我收获颇丰。

## 二、课程注重引导，令人受益匪浅

课程并没有像我想象中的一样，是计算机专业本科课程教学内容的一个压缩版。而是更多地注重引导方面，真正的硬核内容并不多。课程在不同方面起到了引导作用，也让我从根本上认清学了好这样的基础导论课程的重要性。

首先是对正确的价值观的引导，老师在第一节课上就要求我们常看观察者网等网站，关心自己的国家。在课程内容中也贯穿了我国在计算科学领域的成就、现状及未来发展趋势。例如课程中老师分析了国内ICT产业的发展前景，包括新一代通信网络设备、云计算、新型电子元器件和集成电路以及半导体和集成电路产业等。重点讨论了华为、中芯国际等国内知名企业的现状，以及在美国的打压和封锁下的未来发展道路。最后指出未来中美竞争的七条赛道。这大大提高了我对我国相关产业以及国际局势的认识，也让我认识到努力学习，为国家将来科技发展作出贡献的重要性。

其次是对个人能力的引导。作为课程的考核内容之一的分组演讲，要求通过团队合作的方式完成计算领域热点问题的汇报，理解角色任务与团队整体目标，协作完成任务。这不仅锻炼了我的信息检索能力以及PPT制作能力，更是锻炼了我的团队合作能力，在分工合作中我也体会到了团队中成员相互配合的重要性。这些能力在大学生活及未来工作中都是不可或缺的。

最后是对个人未来发展的引导。同样是在课程开始时，老师就要求我们注册了各类计算机论坛及学习平台的账号。强调了信息检索和自主学习的重要性，让我树立起了较强的自主学习和终身学习意识。同时通过分组演讲的选题和个人职业规划的撰写，让我尝试找到了自己感兴趣的方向，并对未来发展作出了规划，这对刚进入大学，对未来人生还较为迷茫的我来说起到了很强的引导作用，为未来个人的发展打下了良好的基础。

## 三、课程内容前沿新颖，拓展视野

作为一门导论课，课程除了介绍计算科学的发展历史之外，还介绍了许多前沿领域的知识，这极大拓展了我的视野。

例如理论方面，课上老师在介绍计算机未来的发展时指出，在摩尔定律越来越难维持、芯片制程已经接近物理极限的今天，发展并行计算技术并不是提高计算机系统性能的根本出路。要想制造出更高性能的计算机，体系结构、部件构成、模型与算法综合考虑都是不可或缺的。又如应用方面，老师介绍了人工智能在数据挖掘、计算机视觉等方面的未来的应用。以及通过虚拟现实VR、增强现实AR，及相关硬件产品微软HoloLens、谷歌眼镜、华为眼镜实施的医疗、军演、办案等多项任务。

通过了解这些计算机领域目前的最新趋势、研究热点和前沿知识，不仅让我对整个行业产生了浓厚的兴趣，更让我对未来发展有了更清晰的认识，也明确了个人职业规划的撰写方向。

# 3 进一步的思考

分组演讲中，我选择了僵尸机这个题目，在阅读了期刊论文《僵尸网络中的关键问题》[1]的基础上制作了PPT,对于其中僵尸网络中的具体检测与反制技术这一问题，我进行了进一步的探索。

### 僵尸网络的检测技术

僵尸网络的检测一直是僵尸网络研究的难点问题，目前主要的检测技术有基于流量分析的检测技术、基于蜜网捕获的检测技术和反向检测技术等。流量分析技术主要是对互联网中某个子网的主机集合实施主动持续监测，蜜网捕获技术对整个互联网进行被动抽样监测，而反向检测技术则根据危害后果反溯僵尸网络。

（一）基于流量分析的检测技术

基于流量分析的检测技术通过对网络数据报文进行持续监测和关联分析来发现僵尸网络的活动。关联分析可以从３个层面进行：纵向关联、横向关联和因果关联。

1. 纵向关联

僵尸程序的多阶段感染过程有一个“基于状态的感染序列模型”，例如目前存在的僵尸结点检测系统BotHunter(参考论文“BotHunter: Detecting malware infection through IDS-driven dialog correlation.”[2])，通过在网关上追踪内部主机与外部网络间的双向通信流量来识别感染过程的不同阶段（包括指向内部网络的扫描、攻击与恶意代码下载，指向外部网络的协同会话、对外攻击与传播等），并将识别结果汇总到关联分析引擎。关联分析引擎对汇总结果进行纵向关联形成可疑会话链，然后与感染序列模型进行匹配以判断是否存在僵尸结点。

这种方法的局限性在于：感染序列模型是预定义的，且对于感染过程各个阶段的检测手段是基于特征的。

1. 横向关联

横向关联检测方法基于如下认识：僵尸结点活动规律是由其共同代码逻辑定义的，因而同一僵尸网络中的结点行为应具有时空相似性．横向关联方法正是通过分析不同主机流量间的时空相似性来检测僵尸结点。基于这种思想实现的系统有BotMiner．BotMiner是一种不限于中心式僵尸网络的通用检测框架，它先分别根据通信流量相似性和恶意行为相似性对主机组进行两维度聚类，然后对聚类结果进行跨维度关联分析，以期发现既具有相似通信模式又具有相似恶意行为模式的主机集合。与BotHunter相比，这种方法的好处是不需要僵尸网络的先验知识（如僵尸程序行为特征等）。

1. 因果关联

上述的两种检测系统都是通过对网络流量的收集分析来发现僵尸结点，另有一种主动探测僵尸网络的系统BotProbe。BotProbe系统基于典型僵尸程序具有确定的命令响应模式且不能容忍会话中发生拼写错误的这一理性认识，利用假设检验的思想，从网络流量中分辨出哪些是僵尸程序与外部的命令与控制会话，哪些是人与人的会话。在检测过程中，BotProbe会向网络中注入一些探针报文，因而是一种主动探测技术．这种方法较之前两种更为积极。

（二）基于蜜网捕获的检测技术

参考论文《蜜网防护系统的研究与实现》[3],基于蜜网捕获的检测技术是指通过设置蜜网系统，对所捕获程序的行为进行分析，判断是否存在僵尸结点。德国的蜜网项目组最早利用蜜网技术对僵尸网络进行检测和跟踪研究，该项目组利用蜜罐蜜网技术捕获了大量僵尸程序，并对这些程序进行了详细研究，为僵尸网络的检测研究提供了第一手资料．蜜网技术本身“守株待兔、愿者上钩”的特点保证了检测结果的准确性，但无法感知不访问蜜网系统的大量恶意代码。

（三）反向检测技术

反向检测技术是指通过对互联网中大规模恶意行为的危害后果进行数据挖掘，寻找隐藏其后的僵尸网络。包括基于时域特征对邮件进行聚类分析、基于邮件外形轮廓特征聚类以检测僵尸网络的方法、基于内容特征的僵尸网络识别系统等等．这种方法基于危害结果进行反溯，针对性较强，结果一般较为可信。

表1：几种僵尸网络检测技术比较

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 方法类型 | 检测系统 | 低误报率 | 高时效性 | 低受限性 |
| 流量分析 | BotHunter等 |  | √ | √ |
| 蜜网捕获 | HoneyBow | √ |  |  |
| 反向检测 | AUTORE |  |  | √ |

### 僵尸网络的反制技术

检测到僵尸网络之后，如何有效反制以缓解或消除其危害，也是僵尸网络研究的一个重要方面，当前的僵尸网络反制技术可以分为网络抑制技术和网络劫持技术两类。

1. 网络抑制技术
2. Sybil攻击技术

参考论文“Sybil Attack Detection Mechanism for Social Networks”[4]，Sybil攻击技术对于非中心式僵尸网络，针对传统P2P网络的攻击技术可以起到反制作用。Sybil攻击有两种方式，一种是内容屏蔽，一种是查询抑制。

内容屏蔽技术首先向僵尸网络中加入一定数量的Sybil结点，使其ID值接近某目标关键字Key；然后Sybil结点在网络中声明自己的存在，试图对多数僵尸结点的路由表造成影响。当僵尸网络节点结点查询该关键字Key时，就有可能被误导到Sybil结点，从而屏蔽真实搜索目标。

查询抑制是指利用查询停止机制，令Sybil在收到任何查询请求时，都向请求结点返回特定信息以使其停止进一步搜索，导致请求结点无法获得目标信息。因此Sybil攻击技术是抑制P2P僵尸网络的有效手段。

1. 内容污染技术

内容污染技术主要用于非中心式的僵尸网络，通过覆盖目标结点中所存储的命令与控制信息，阻止命令与控制信息在僵尸网络中传播。在僵尸网络中，为阻止以关键字Key为索引的命令与控制信息在网络中传播，内容污染技术首先搜索所有可能存储了该信息的结点，然后重新构造以Key为索引的假信息并以一定的频率反复地向这些结点发布，覆盖原有信息。在能够获得命令与控制信息发布规律的情况下，内容污染方法是一种高效的抑制手段。

（3）结点清除技术

清除僵尸网络结点可以达到直接抑制僵尸网络的效果．僵尸网络结点清除有３种策略：定向清除、树形清除和随机清除。

定向清除按照连接度由高到低的顺序清除僵尸网络结点，这种方式对中心式僵尸网络的抑制效果显著，通过直接停止中心服务器的运转或者联系域名服务商拒绝对僵尸网络提供服务，可以达到瘫痪僵尸网络的目的。

树形清除，是防护方利用已经捕获的僵尸结点，分析出与之有连接关系的其他僵尸结点，“顺藤摸瓜”地进行结点清除。

随机清除指随机地对僵尸网络中的结点进行清除，僵尸网络的结点被宿主机用户或杀毒软件发现并查杀，是随机清除的典型情况。

1. 网络劫持技术
2. 域名抢注

很多中心式僵尸网络为了提高隐蔽性，会频繁更换其中心服务器的域名，这就为劫持僵尸网络提供了机会．通过分析僵尸程序，可以获得其中心服务器域名变换规律，通过预测并抢注其中心服务器将要采用的域名，使僵尸结点误将防护方的服务器作为其中心服务器，并接受其指令。由于不少僵尸网络都设计有自卸载功能，因此在劫持这类僵尸网络后，可以通过发布自卸载命令来高效清除宿主机器上的僵尸程序。

1. Sybil欺骗

在P2P僵尸网络中，Sybil结点如果对任何僵尸结点的搜索请求返回特意构造的信息，就有可能实现对僵尸网络的劫持。

1. 内容替换

参考论文《基于流量的P2P僵尸网络检测》[5]，在对P2P僵尸网络的抑制技术中，内容污染通过将被目标关键字索引的内容都覆盖掉，导致僵尸网络无法有效传递命令与控制信息。如果使用特意构造的信息来覆盖目标内容，僵尸结点在获取并执行相应命令后，就有可能被劫持。

表2：僵尸网络反制技术比较

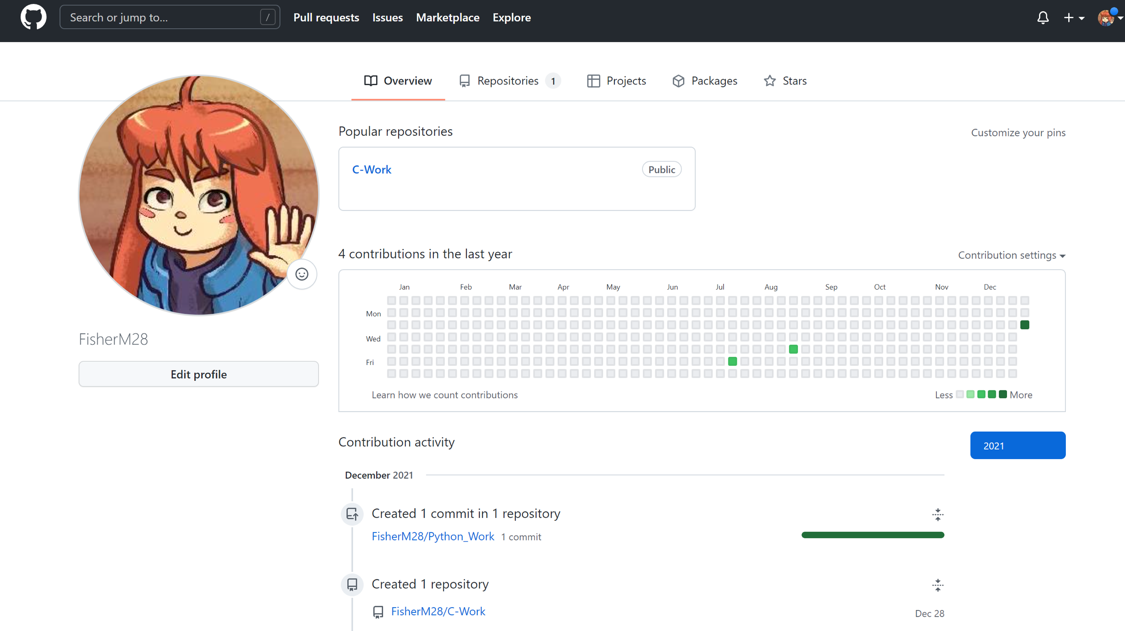
|  |  |  |  |
| --- | --- | --- | --- |
| 方法类型 | 反制技术 | 中心式适用 | 非中心式适用 |
| 网络抑制 | Sybil攻击 |  | √ |
| 内容污染 |  | √ |
| 结点清除 | √ | √ |
| 网络劫持 | 域名抢注 | √ |  |
| Sybil欺骗 |  | √ |
| 内容替换 |  | √ |

# 4 总结

通过对计算科学导论这门课程的学习和课程总结报告的撰写，我不仅对计算科学以及未来的学习工作生活有了一个整体的认识，更是丰富了自己的科学思维，锻炼了我的包括团队合作能力在内的许多能力，可以说收获颇丰。相信在未来，我在这门课上学到的知识一定会伴我终生，在许多方面给予我帮助。

# 5 附录

## Github

<https://github.com/FisherM28>

## 观察者

## IMG_5095

## 学习强国

## 图片2

## 哔哩哔哩



## CSDN

<https://blog.csdn.net/FisherM28>

## 博客园

https://home.cnblogs.com/u/2705231



## 小木虫

注册小木虫账户，给出个人网址和个人网站截图

<http://muchong.com/bbs/space.php?uid=28050172>



# 参考文献

1. 王天佐,王怀民,刘波,史佩昌.僵尸网络中的关键问题[J].计算机学报,2012,35(06):1192-1208.

[2]Gu Guofei, Porras Philip, Yegneswaran Vinod, Fong Martin. BotHunter: Detecting malware infection through IDS-driven dialog correlation. Boston, USA, 2017: 167-182.

[3]游杰,汤辉,李书锋.蜜网防护系统的研究与实现[J].江西通信科技,2021(01):41-42.DOI:10.16714/j.cnki.36-1115/tn.2021.01.014.

[4]Bharathi, A,Priyanka, D. Yazhini,Padmapriya, P,Priyadharsnee, K. Robust Sybil Attack Detection Mechanism for Social Networks[J]. Journal of Computational and Theoretical Nanoscience,2018,15(5):

[5]李建.基于流量的P2P僵尸网络检测[J].计算机时代,2016(05):45-48.DOI:10.16644/j.cnki.cn33-1094/tp.2016.05.012.