[论文阅读] (12)英文论文引言introduction如何撰写及精句摘抄——以入侵检测系统(IDS)为例

原创 Eastmount 于 2021-11-23 13:40:11 发布 10067 已收藏 17 编辑 版权
分类专栏： 娜璋带你读论文 文章标签： 论文撰写 引言 入侵检测 网络安全 SCI

娜璋带你读论文 专栏收录该内容 167 订阅 26 篇文章

《娜璋带你读论文》系列主要是督促自己阅读优秀论文及听取学术讲座，并分享给大家，希望您喜欢。由于作者的英文水平和学术能力不高，需要不断提升，所以还请大家批评指正，非常欢迎大家给我留言评论，学术路上期待与您前行，加油。

前一篇文章详细介绍ACE去雾算法、暗通道先验去雾算法以及雾化生成算法，并且参考了两位计算机视觉大佬（Rizzi 何恺明）的论文。这篇文章将从个人角度介绍英文论文引言如何撰写，一方面自己英文太差，只能通过最土的办法慢慢提升，另一方面是自己的个人学习笔记，并分享出来希望大家批评和指正。希望这篇文章对您有所帮助，这些大佬是真的值得我们去学习，献上小弟的膝盖~fighting！

这里选择的论文多数为近三年的CCF A和二区以上为主，尤其是顶会顶刊。当然，作者能力有限，只能结合自己的实力和实际阅读情况出发，也希望自己能不断进步，每个部分都会持续补充。可能五年十年后，也会详细分享一篇英文论文如何撰写，目前主要以学习和笔记为主。大佬还请飘过O(∩_∩)O

文章目录

前文赏析：

- [论文阅读] (01) 拿什么来拯救我的拖延症？初学者如何提升编程兴趣及LATEX入门详解
- [论文阅读] (02) SP2019-Neural Cleanse: Identifying and Mitigating Backdoor Attacks in DNN
- [论文阅读] (03) 清华张超老师 - GreyOne: Discover Vulnerabilities with Data Flow Sensitive Fuzzing
- [论文阅读] (04) 人工智能真的安全吗？浙大团队外滩大会分享AI对抗样本技术
- [论文阅读] (05) NLP知识总结及NLP论文撰写之道——Pvop老师
- [论文阅读] (06) 万字详解什么是生成对抗网络GAN？经典论文及案例普及
- [论文阅读] (07) RAID2020 Cyber Threat Intelligence Modeling Based on Heterogeneous GCN
- [论文阅读] (08) NDSS2020 UNICORN: Runtime Provenance-Based Detector for Advanced Persistent Threats
- [论文阅读] (09)S&P2019 HOLMES Real-time APT Detection through Correlation of Suspicious Information Flow
- [论文阅读] (10)基于溯源图的APT攻击检测安全顶会总结
- [论文阅读] (11)ACE算法和暗通道先验图像去雾算法（Rizzi | 何恺明老师）
- [论文阅读] (12)英文论文引言introduction如何撰写及精句摘抄——以入侵检测系统(IDS)为例

一.引言如何撰写

论文如何撰写因人而异，作者仅分享自己的观点，欢迎大家提出意见。然而，坚持阅读所研究领域最

新和经典论文，这个大家应该会赞成，如果能做到相关领域文献如数家珍，就离你撰写第一篇英文论文更近一步了。重点是多读多写，共勉！

1.论文总体框架及引言撰写

该部分回顾和参考周老师的博士课程内容，感谢老师的分享。典型的论文框架包括两种（The typical “anatomy” of a paper），如下所示：

第一种格式：理论研究

- **Title and authors**
- **Abstract**
- **Introduction**
- **Related Work** (可置后)
- **Materials and Methods**
- **Results**
- **Acknowledgements**
- **References**

第二种格式：系统研究

- **Title and authors**
- **Abstract**
- **Introduction**
- **Related Work** (可置后)
- **System Model**
- **Mathematics and algorithms**
- **Experiments**
- **Acknowledgements**
- **References**

引言主要为提供领域背景信息，以理解为什么从事该研究。

- Presents the background information for a fellow scientist (possibly in another field) to understand why the findings of this paper are significant.

引言的结构通常是：

- **Accepted state of knowledge in the field**
  领域背景知识
- **Focus on a particular aspect of the field**
  聚焦领域
- **The research problem the paper attempts to address**
  研究问题解决情况
- **methodology / approach**
  提出方法
- **Conclusions** (scientists don’t really like surprise endings!)
  结论及贡献（contributions）

那么，如何撰写引言呢？下面是课堂练习。

- Grab a blank piece of paper:
  – Take notes
  – Draw mini figures
  – Define vocabulary
  (wikipedia is a quick reference)
- Answer these questions:
  – What is the research problem the paper attempts to address?
  – What are the claimed contributions of the paper?
  – How do the authors substantiate their claims?
  – What are the basic conclusions? (Scientists don’t really like surprise endings and this is usually stated in the last paragraph.)

2.引言撰写

该部分主要是学习易莉老师书籍，具体如下：

引言（Introduction）无疑是整篇论文里最难的部分之一。前言的作用主要是为读者理解文章的贡献提供一个背景，让读者了解：

- 这个研究的主要研究问题是什么？它有怎么的重要性？
- 这个问题前人研究、解决到了什么程度？领域内没有解决的问题或者有争论的地方在哪里？
- 本研究主要用什么方法来研究这个问题（对研究方法做个概括）？其预期结果是什么？

- 本研究的创新点主要是什么？其优势突出在哪里？

《10条简单规则》一文建议，引言应该充宏大的角度来切入，然后议题缩小到文章讨论的问题范畴内。下一篇会介绍“如何讲好故事”详细讲解，这里我们需要知道讲故事的方式、层次以及深度都要由文章的目的以及预计发表期刊\会议的性质决定。

比如“入侵检测系统”会发表在安全或计算机等领域期刊或会议上，所以需要论述网络空间安全、APT攻击、入侵检测系统、恶意流量检测相关的背景知识。 **建议越早引入研究问题越好，如有可能，在第一段结尾就亮出研究问题，这样读者可以更有针对性地理解前言和文章的剩余部分。**

> 例如：… In this study, we investigated how children with ASD attribute false belief to a social robot.

研究问题的提出，通常需要在总结前人研究的基础上，提出前人研究没有解决的问题，或者尚存在争议的问题。因为只有说明你的研究能更好地理解这些没有解决好的问题，才能体现出创新性，否则无法体现你的研究贡献。 **这里要特别注意，不要评判别人的研究（用一些“poor” “unreliable”这样的形容词），也不要给自己贴金（“the first to” “more advanced”，以及中文常见的“填补空白”）。注意把握语音的分寸，客观地论述自己的贡献，让读者来评判。**

3.个人理解

个人感觉：良好的开端等于成功的一半，引言决定了读者或审稿老师对你论文的第一印象。论文的引言真的非常重要，好的引言决定一篇文章的上限，尤其是审稿老师审稿时（由于研究领域的差异性），重点会阅读引言，一个“完美”的引言会让读者或评阅者有继续阅读和欣赏的意愿，会让读者或评阅者思考你提出的观点，并想知道你将如何证明你的论点。这也从侧面上体现了文章的整体价值。

因此，如何写好引言，写高质量引言，写引人入胜的引言很关键。

引言撰写需要注意：

- 开篇角度要尽量放宽然后缩小范围，篇幅内容要适宜。引言的开头可以相对宽泛地介绍研究背景，但最终一定要与你的研究有关系。
- 提出研究目的和意义，引言的主要作用是介绍相关研究背景和你所研究的课题，现象或观点，在引言中要提出你的论点，即本文的方法及贡献。
- 审稿专家将在引言中快速寻找几个问题：文章的工作是否新颖？科学贡献是否重要？文章质量是否适合在本期刊发表？
- 充分引用但不滥用引文。聚焦到该研究主题后，应该充分涵盖最新的相关文献。文献综述应该完整，但不能冗长（非综述），同时避免在单一观点上引用过多文献。

- 避免过多的细节描述。在引言中，如果你的论文在介绍方法之前大量地概括研究主要成果，那么应该避免陈述太多详细的结果。
- 引言回溯法，可以选择先进行文章正文的写作，再进行引言的撰写。有了一定的思路、论据和结构后，引言撰写会更得心应手。
- 结合投稿会议或期刊要求进行撰写。
- 多读（顶会论文）多写，实践最重要。

个人喜欢将引言分为以下几个部分，当然不同的类型写法也不尽相同，如综述、理论、系统、方法论等。

- **第一部分：从现实背景引入到该研究问题至关重要**
  对所研究的大领域进行陈述，这样的陈述提供了一个背景，使读者对研究的问题及其重要性有一个大致了解。
- **第二部分：解释研究问题（xxx旨在完成xxx），介绍近年来取得的研究进展（顶会和顶刊为主），通过“然而”引出当前方法存在的问题**
  前人对相同问题在不同方面做过的研究，要对这些已有研究做更加具体的陈述，从而建立一个包含已有知识和信息的基础。同时，指出需要更多的研究来弥补空白（gap），或者拓展已有的研究。
- **第三部分：本文拟提出的方法，从哪些方面如何解决该问题，如何解决上述问题**
  非常具体的陈述指出本文的研究目的，主要的研究工作或结果。
- **第四分布：本文的主要贡献**
  对于开展本研究的作用、贡献和重要性的陈述，对文章接下来内容的概述（可省略）。

此外，引用部分的关键词也非常重要，良好的关键词起到承上启下的作用。我们需要将所有环节结合在一起形成一个逻辑连贯的“引言”。同时，你可能需要再添加少量的句子来提供研究背景（比如与主题相关的网络安全攻击事件，Stuxnet、WannaCry等），或者再次安排一下有些句段来使逻辑流动的更加顺畅。这样不仅展示出清晰的写作思路，更让读者能够轻松的读懂你的表达。

该部分参考资料：

- [1] 易莉. 学术写作原来是这样[M]. 机器工业出版社.
- [2] 仓岛保美 甘菁菁. 写作的逻辑[M]. 人民邮电出版社.
- [3] Ruiting Zhou. 博士英语课程学习心得. 武汉大学(周老师).
- [4] Kelly Hogan. how to read a scientific paper
- [5] Philip W. L. Fong. How to Read a CS Research Paper?
- [6] 知乎. 怎么写好论文引言？. https://www.zhihu.com/question/57366545
- [7] 知乎. 如何撰写高分引言？. https://zhuanlan.zhihu.com/p/165505555

二.入侵检测系统论文引言句子

个人习惯将引言分为四部分介绍，也欢迎大家批评指正。下面主要以CCF A会议和期刊论文为主进行介绍，重点以入侵检测系统（Intrusion Detection System，IDS）领域为主。

第1部分：背景介绍和引入

Traditional malicious traffic detection identifies malicious traffic by analyzing the features of traffic according to preconfigured rules, which aims to protect legitimate Internet users from network attacks [29, 47]. However, the rule-base detection is unable to detect zero-day attacks [8, 12, 22, 65] though it can achieve high detection accuracy and detection throughput in high bandwidth networks, e.g., in Internet backbone networks.

传统IDS旨在…然而…

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

The increasing scale and complexity of modern networks and the tremendous amount (大量) of applications running on them render communication and networking systems highly vulnerable to various intrusion attacks. Intrusion detection system (IDS) plays a significant role in safeguarding networks from intrusion attacks.

With the rapid advancement in machine learning (ML), ML-based Intrusion Detection Systems (IDSs) are widely deployed to protect networks from various attacks.

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

The mass adoption of IoT technology in smart homes has made them attractive targets to cyber threats, from unlocking doors and eavesdropping on occupants through their own cameras to hijacking (劫持) voice-controlled personal assistant devices.

- Ryan Heartfield, et al. Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. IEEE TIFS.

The electricity grid is a highly complex control system and is one of the most impressive engineering feats of the modern era. Modern societies critically rely on the proper operation of power delivery systems in nearly every facet [1]–[3].

There are a number of threats to the reliability and security of the electric grid, including space weather, aging, accidents, and random failures. In this paper, we focused on the growing threat from cyberattacks to substations.

- Tohid Shekari, et al. RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid. NDSS.

The unprecedented (前所未有的) evolution of networks with a growing plethora of connected devices and things are reshaping the landscape of an Internet-of-Things (IoT). Ranging from devices such as indoor or outdoor surveillance cameras, electrical and mechanical appliances, mobile user-worn devices such as smart watches or health monitors, to connected vehicles and vehicular components, industrial systems, and connected smart cities, the IoT landscape is continuously evolving (see Fig. 1).

Due to the increasing diversity of devices, networks and services in an IoT ecosystem, the

vulnerabilities of each constituent technology could be agglomerated, giving rise to novel threats and attack vectors.

- Abdul Jabbar Siddiqui, et al. TempoCode-IoT: temporal codebook-based encoding of flow features
  for intrusion detection in Internet of Things. Cluster Computing.

The ADVENT of Internet-of-Things (IoT) systems and their ongoing convergence with diverse industry applications signifies the imminent next wave of the ubiquitously connected society [1]–[5]. By interconnecting different objects (i.e., things), distributed data associated with one industry or business process in the physical world, for example, temperature, humidity, and traffic information over a large area can be collected by different sensors. Accurate and trustworthy collection of such data [6]–[10] play an important role in decision making for smart IoT applications, especially for those industry applications relying on tight collaboration among diverse entities, and they are expected to provide a multitude of different domains of smart services, ranging from environmental monitoring, infrastructure monitoring, to smart factory, just to name a few [11].

- Zhenlong Xiao, et al. Anomalous IoT Sensor Data Detection: An Efficient Approach Enabled by Nonlinear Frequency-Domain Graph Analysis. IOTJ

However, those resource-constraint IoT sensors could be compromised easily, leading to the anomalous data in IoT systems by false-data-injection attacks [12]–[16]. Such anomalous sensor data may result in erroneous decision making and further cause cascaded system failure and avalanche-like reaction due to the extremely high complexity and interdependency among different components of large-scale IoT systems. Hence, the anomalous data detection from the collected sensor data is extremely important for IoT-based smart applications.

- Zhenlong Xiao, et al. Anomalous IoT Sensor Data Detection: An Efficient Approach Enabled by Nonlinear Frequency-Domain Graph Analysis. IOTJ

With advances in network-based computing services and applications, the Internet suffers from more and more security threats. Therefore, intrusion detection systems (IDS) are particularly important as an essential part of network security defense. IDS discovers and identifies intrusions in the system by detecting and analyzing network traffic or host behaviors.

- Xinghua Li, et al. Sustainable Ensemble Learning Driving Intrusion Detection Model. TDSC.

Network Intrusion Detection System (NIDS) is a critical network security function that is designed to monitor the traffic in a network to detect malicious activities or security policy violations. Recently, lots of networks have reached the throughput of 100 Gbps [83]. To keep up with the pace of the soaring throughput of networks, multi-thread approaches [35, 77] have been proposed to build NIDSes to meet the high throughput requirement for detecting attacks. In addition, some NIDSes, such as Bro [67], can be deployed as NIDS clusters [81] that spread detection tasks across multiple nodes.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

However, despite their usefulness in addressing scalability issues for NIDSes, both multi-thread and cluster solutions remain limited in flexibility regarding the processing capacity and placement location. In particular, they are still inflexible to detect attacks when a significant workload spike happens. For example, a massive attack like DDoS could bring the network traffic volume up to 500 GBps [42], which requires the NIDSes scaling accordingly to process the peak traffic load.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

Moreover, these approaches are also inflexible to protect current prevailing virtualized environments, because the perimeters of networks in virtualized environments become blur and fluid, where applications may migrate from one physical machine to another within a data center or even across multiple data centers for the purpose of flexible resource management and optimization [31]. Therefore, improving the design of current NIDSes to make them well suited to provide flexible network intrusion detection is urgent and relevant.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

Cyber-physical systems (CPS) are increasingly being deployed in critical infrastructures. The CPS market is expected to expand by 9.7% each year, which will reach $9,563M by 2025 [82]. Prominent applications of CPS include industrial control systems (ICS), smart grid, intelligent transportation systems (ITS), and aerial systems. CPSs have evolved to be complex, heterogeneous, and integrated to provide rich functionalities. However, such characteristics also expose CPSs to broader threats.

- Yuan LUO, et al. Deep Learning-based Anomaly Detection in Cyber-physical Systems:

Progress and Opportunities. ACM Computing Surveys.

A variety of services have been proposed using Internet of Things (IoT) devices. IoT devices have been one of the frequent targets for adversaries because they are generally cheap with a lack of security awareness. One of the security mechanisms is the intrusion detection systems (IDSes) for detecting on-going intrusions in such IoT networks. There are mainly two types of IDS: network-based intrusion detection system (NIDS) and host-based intrusion detection system (HIDS). Unlike HIDS which is specialized in detecting attacks within a single device, NIDS analyzes data traffic in a networked system to discover the existence of attacks. NIDS has been preferred by researchers for IoT security [1], [10], [11] because an IoT system can be viewed not as a standalone computing device but as a cluster of devices networked to form an ecosystem.

- Sunwoo Ahn, et al. Hawkware: Network Intrusion Detection based on Behavior Analysis with ANNs on an IoT Device. DAC.

HOST-BASED intrusion detection has long been an important measure to enforce computer security. In today's world, the cyber attack has become a persistent, aggressive and disruptive threat. For instance, the Advanced Persistent Threat (APT) attack has gradually become a main threat in enterprise's environment [1], [2]. The "WannaCry" virus has attacked nearly 100 countries in the world [3] and resulted in huge economic losses in 2017 [4].

- Yulai Xie, et al. Pagoda: A Hybrid Approach to Enable Efficient Real-Time Provenance Based Intrusion Detection in Big Data Environments. IEEE Transactions on Dependable and Secure Computing.

WITH the increasing popularity of the Internet in modern life, a larger number of devices have become interoperable through networks, and the security of cyberspace has attracted greater attention. Intrusion detection systems (IDSs) are used to detect various malicious attacks on a network effectively and are one of the most critical systems for maintaining cyberspace security [1]. From the perspective of machine learning (ML), an IDS can be defined as a system aimed to classify network traffic.

- Congyuan Xu, et al. A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework. IEEE Transactions on Information Forensics and Security.

第2部分：研究主题及相关工作介绍

The goal of ML-based IDS is to learn a decision boundary that discriminates (区分) malicious

network traffic from benign network traffic.

ML technologies have seen great success in domains such as computer vision and natural language processing. While applying to network intrusion detection, state-of-the-art IDSs usually implement advanced neural networks (e.g., LSTM) and learning schemes (e.g., meta-learning and active learning).

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

In light of these incidents, researchers in academia and industry are gearing efforts to develop novel solutions for intrusion detection in IoT, to secure IoT from different types of intrusions [8, 32, 37, 39]. The various IDSs could be broadly classified in terms of their placement strategy as: centralized, distributed, or hybrid.

- Abdul Jabbar Siddiqui, et al. TempoCode-IoT: temporal codebook-based encoding of flow features
  for intrusion detection in Internet of Things. Cluster Computing.

To achieve this purpose, intrusion detection systems (IDSs) (Scarfone and Mell, 2007) are a basic and important security mechanism to defend IoT environments against various security threats. Traditionally, an IDS can be classified into two categories: signature-based IDS and anomaly-based IDS. The former like (Vigna and Kemmerer, 1998; Roesch, 1999) detects a potential threat by comparing inputting events (e.g., system logs) with known signatures, which are used to describe a known attack by means of expert knowledge. By contrast, the latter (Valdes and Anderson, 1995; Ghosh et al., 1998) identifies great deviations between existing events with the pre-established normal profile.

- Wenjuan Li, et al. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications.

A significant amount of research has been conducted to develop intelligent intrusion detection techniques, which help achieve better network security. Bagged boosting-based on C5 decision trees [2] and Kernel Miner [3] are two of the earliest attempts to build intrusion detection schemes. Methods proposed in [4] and [5] have successfully applied machine learning techniques, such as Support Vector Machine (SVM), to classify network traffic patterns that do not match normal network traffic.

- Mohammed A. Ambusaidi, et al. Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. IEEE TRANSACTIONS ON COMPUTERS

In order to detect abnormal behaviors in large-scale network traffic, machine learning-based intrusion detection systems [1], [2], [3] have attracted a wide range of attention. Such methods adopt machine learning techniques to extract features from a large amount of data and train a classification model to classify network traffic or host behaviors to detect intrusions in the system. In order to reduce the false alarm rate and false negative rate, prior works on the machine learning-based intrusion detection system often employ multiple machine learning models [4], [5], [6] to construct the detection model, called ensemble learning method, as demonstrated in Fig. 1.

- Xinghua Li, et al. Sustainable Ensemble Learning Driving Intrusion Detection Model. TDSC.

In this work, our goal is to make a step towards elastic security through NIDS virtualization that overcomes the inflexibility of current NIDS architectures. The virtualization of NIDSes must be safe and efficient. The safe virtualization requires that virtualized NIDSes do not miss any potential attacks that can be detected by traditional NIDSes. The efficient virtualization requires that virtualized NIDSes are provisioned optimally and consume minimum resources.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

Current practise for securing organizational networks is to rely on Intrusion Detection Systems (IDS) that inspect network traffic to detect attacks. However, such solutions are either extremely expensive if they are hardware-based, or unscalable to high datarates if they are software-based. Further, the myriad variety of IoT devices, each with its own specific behavior and security vulnerabilities, makes it challenging for the IDS to distinguish normal from abnormal traffic that could be symptomatic of an attack.

- Ayyoob Hamza, et al. Combining MUD Policies with SDN for IoT Intrusion Detection. IOT S&P.

The traditional intrusion detection system typically uses system calls to analyze and identify host-based intrusion [5], [6], [7], [8], [9], [10]. However, these methods are not widely used. Since they do not disclose how the intrusion happens, and thus the detection accuracy is not high. With the stealth and sophistication of modern attacks, it's critical to identify the causality relationships between the intruder and the damaged files. The existing mainstream methods focus on offline forensic analysis using provenance [11], [12] or audit logs [13], [14], [15]. However, typical attacks such as APT can remain stealthy for half a year after getting into the enterprise [16]. It is too late if sensitive data have been stolen before disclosing the intrusion source.

- Yulai Xie, et al. Pagoda: A Hybrid Approach to Enable Efficient Real-Time Provenance Based Intrusion Detection in Big Data Environments. IEEE Transactions on Dependable and Secure Computing.

A simple model is a binary classification one, which is used to distinguish between the normal and malicious network traffic, thereby enabling the detection of intrusion traffic. With recent advances in research focused on ML, many studies have shown that it is possible to design ML algorithms with the purpose of implementing IDSs. These algorithms are generally no longer based on rules and are aimed to exploit various features of network traffic. They comprise two main steps: feature extraction and classification. For example, in the research work [2], a method of encoding the payload was proposed based on recursive feature addition (RFA) and bigram, and then was utilized to detect intrusions. The experimental results on the ISCX2012 dataset demonstrated that the detection rate could reach 89.60%.

- Congyuan Xu, et al. A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework. IEEE Transactions on Information Forensics and Security.

第3部分：现有方法存在的缺陷

通过现有方法存在缺陷引出本文的方法。

There are mainly two types of IDS: signature-based detection [2] and anomaly-based detection [3]. Signature-based detection schemes work by extracting the traffic signature and comparing to those in a pre-built knowledge base. As a result, they are only effective in detecting known attacks but cannot detect attacks outside the knowledge base. Anomaly-based detection aims to detect deviations from an established norm traffic model.

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

Compared with rule based methods, machine learning based methods can effectively identify zero-day malicious traffic [12, 22]. Unfortunately, due to the processing overhead of machine learning algorithms, existing detection methods achieve low detection throughput and are unable to process high-rate traffic. As a result, most of these methods can only be deployed offline [2, 4, 5, 15, 28, 49] so that they cannot realize realtime detection, particularly in high performance networks (e.g., in 10 Gigabit networks) [42, 77, 78].

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

Meanwhile, attackers can easily interfere with and evade these methods by injecting noises, e.g., packets generated by benign applications, into attack traffic. Packet-level detection [42, 53, 68] that analyzes per-packet feature sequences is unable to achieve robust detection. Actually, even in the absence of the evasion attacks, the packet-level detection is unable to detect sophisticated zero-day attacks. Traditional flow-level methods [4, 28, 49, 77] detecting attacks by analyzing flow-level statistics incur significant detection latency. Moreover, evasion attacks can easily bypass the traditional flow-level detection that uses coarse-grained flow-level statistics [14, 63]. Thus, realtime robust machine learning based detection that is ready for real deployment is still missing.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

Smart homes, however, present unique challenges with very specific requirements that can make generalist approaches unsuitable (通用方法不适用).

- Ryan Heartfield, et al. Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. IEEE TIFS.

To detect attacks early and potentially reduce their damaging consequences, we need a reliable and robust intrusion detection system (IDS) for the power grid. The existing IDSs focused on securing power substations through monitoring the network traffic of the SCADA system. Accordingly, if the attacker can compromise the SCADA network entirely, the IDS will not be able to detect his malicious activities in the substation.

Motivated by this fact, the aim of this paper is to propose an air-gapped distributed IDS which monitors the substation activities by radio frequency (RF) measurements (as a side channel) to verify the correctness of the SCADA network traffic. With this approach, the SCADA system is assumed to be an untrusted entity.

- Tohid Shekari, et al. RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid. NDSS.

However, current network traffic data, which are often huge in size, present a major challenge to IDSs [9]. These “big data” slow down the entire detection process and may lead to unsatisfactory classification accuracy due to the computational difficulties in handling such data. Classifying a huge amount of data usually causes many mathematical difficulties which then lead to higher computational complexity.

- Mohammed A. Ambusaidi, et al. Building an Intrusion Detection System Using a Filter-Based

Feature Selection Algorithm. IEEE TRANSACTIONS ON COMPUTERS

To detect attacks and unexpected errors in CPSs, anomaly detection methods are proposed to mitigate these threats. For example, rule, state estimation (e.g., Kalman filter), and statistical model (e.g., Gaussian model, histogram-based model) based methods are utilized to learn normal status of CPSs [65]. However, these methods usually require expert knowledge (e.g., operators manually extract certain rules) or need to know the underlying distribution of normal data. Machine learning approaches do not rely on domain-specific knowledge [18]. But they usually require a large quantity of labeled data (e.g., classification-based methods). Also, they cannot capture the unique attributes of CPSs (e.g., spatial-temporal correlation) [88].

- Yuan LUO, et al. Deep Learning-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities. ACM Computing Surveys.

Intrusion detection methods are dedicated to ensuring network communication security [70, 116]. Physical properties are captured to depict the immutable nature of CPSs [36]. Program execution semantics are characterized to protect control systems [19, 89, 112]. However, as CPSs become more complicated and attacks are more stealthy (e.g., APT attacks), these methods are hard to ensure the overall status of CPSs (e.g., protect multivariate physical measurement) and need more domain knowledge (e.g., more components and correlation). Anomaly detection systems need to adapt to capture new characteristics of CPSs.

- Yuan LUO, et al. Deep Learning-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities. ACM Computing Surveys.

The aforementioned works demonstrate that for a specific type of attack, as long as there is a large number of samples, many ML algorithms can perform appropriately, and detection can be completely automated, no longer requiring excessive manual intervention. It can be outlined that IDSs based on ML can detect new attacks as long as the number of samples for training is sufficient. However, at present, the cyberspace environment is constantly changing, and new types of attacks occur constantly. For example, the zero-day attack [14] is an attack launched on the day when a vulnerability is discovered. It is difficult for security agencies to obtain sufficient attack samples in a short period, and as a result, it may be too late to compose a dataset and publish it.

- Congyuan Xu, et al. A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework. IEEE Transactions on Information Forensics and Security.

第4部分：本文方法及贡献

(1) 本文方法

In this paper, we develop Whisper that aims to realize realtime robust malicious traffic detection by utilizing machine learning algorithms. Whisper effectively extracts and analyzes the sequential information of network traffic by frequency domain analysis [51], which extracts traffic features with low information loss. Especially, the frequency domain features of traffic can efficiently represent various packet ordering patterns of traffic with low feature redundancy.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

To effectively perform frequency domain traffic feature analysis, we develop a three-step frequency domain feature extraction. First, we encode per-packet feature sequences as vectors, which reduces the data scale and the overhead of subsequent processing. Second, we segment the encoded vectors and perform Discrete Fourier Transformation (DFT) [51] on each frame, which aims to extract the sequential information of traffic. It allows statistical machine learning algorithms to easily learn the patterns. Third, we perform logarithmic transformation on the modulus of the frequency domain representation produced by DFT, which prevents float point overflows incurred by the numerical instability issue [23] during the training of machine learning.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

Furthermore, we propose an automatic parameter selection module to select the encoding vector for efficient packet feature encoding. To achieve this, we formulate the per-packet feature encoding as a constrained optimization problem to minimize mutual interference of the per-packet features during frequency domain feature analysis.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

In this paper, we propose MANDA, a MANifold and Decision boundary-based AE detection scheme for ML-based IDS.

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

In addition, MAGPIE introduces three more innovations (创新) to ensure its practicality in a household, including taking into account users' risk tolerance, human presence and cyber-physical sources of data. In summary, MAGPIE implements the following contributions:

- Ryan Heartfield, et al. Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. IEEE TIFS.

In order to address the problem of intrusion attacks in IoT, this work proposes a novel method to detect intrusions by transforming flow-based features into more discriminative representations and designs an ensemble of classifiers based on these to differentiate between benign and malicious flows. The proposed method is designed to serve in a centralized IDS, leveraging the compute and storage resources therein. The main contributions of this work are summarised as follows:

- Abdul Jabbar Siddiqui, et al. TempoCode-IoT: temporal codebook-based encoding of flow features
  for intrusion detection in Internet of Things. Cluster Computing.

Due to such merits, in this work, our main purpose is to apply the disagreement-based method to intrusion detection. We particularly devise a simple disagreement-based semi-supervised learning algorithm and investigate its performance of detecting intrusions. In addition, due to the nature of IoT networks, there is a need to deploy collaborative intrusion detection systems (CIDSs) to protect the distributed environment. Motivated by this, we further design DAS-CIDS to investigate the use of disagreement-based semi-supervised learning in CIDSs, in the aspects of detection improvement and alarm filtration. The contributions of this work can be summarized as below.

- Wenjuan Li, et al. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications.

To address the aforementioned problems on the methods for feature selection, we have proposed a Hybrid Feature Selection Algorithm (HFSA) in [10]. HFSA consists of two phases. The upper phase conducts a preliminary search to eliminate irrelevant and redundant features from the original data. This helps the wrapper method (the lower phase) to decrease the search range from the entire original feature space to the pre-selected features (the output of the upper phase). In this paper, we extend our work discussed in [10]. The key contributions of this paper are listed as follows.

- Mohammed A. Ambusaidi, et al. Building an Intrusion Detection System Using a Filter-Based

Feature Selection Algorithm. IEEE TRANSACTIONS ON COMPUTERS

Therefore, the existing solutions are difficult to adapt to the characteristics of attack diversity and dynamic time-variation. To solve the above problems, this paper proposes an intrusion detection model based on sustainable ensemble learning. The main contributions are summarized as follows:

- Xinghua Li, et al. Sustainable Ensemble Learning Driving Intrusion Detection Model. TDSC.

In this paper, we propose a novel NIDS architecture, vNIDS, which enables safe and efficient virtualization of NIDSes. To address the effective intrusion detection challenge, we classify detection states of virtualized NIDSes into local and global detection states to minimize the number of detection states shared between instances.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

To this end, deep learning-based anomaly detection (DLAD) methods have been proposed to identify anomalies in CPS. Current studies have explored different neural network architectures (e.g., ConvLSTM) to mitigate various threats (e.g., false data injection attacks) in different CPS domains (e.g., smart grid). However, since these studies are not introduced in a unified way, a systematic survey is needed to review existing methods and provide guidance for future solutions. Specifically, we need to answer the following four research questions:

- Yuan LUO, et al. Deep Learning-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities. ACM Computing Surveys.

To resolve these issues, we propose, Hawkware, our lightweight ANN-based distributed NIDS that detects attacks on a device without actual data analysis for DPI, yet attaining better accuracy than latest NIDS [1] for IoT devices. Since resource consumption is a primary concern of every embedded device in an IoT system, efficiency must be of top priority for any techniques targeting most embedded devices with strict resource constraints.

- Sunwoo Ahn, et al. Hawkware: Network Intrusion Detection based on Behavior Analysis with ANNs on an IoT Device. DAC.

In this paper we aim to increase the scalability and efficacy of IDS using a combination of MUD and SDN. Manufacturer Usage Description (MUD) [12] is an emerging IETF framework for formally specifying the expected network behavior of an IoT device. IoT devices generally

perform a specific function, and therefore have a recognizable communication pattern [16], which can be captured formally and succinctly as a MUD profile. Using the Software Defined Networking (SDN) paradigm, this formal behavioral profile can be translated to static and dynamic flow rules that can be enforced at run-time by the network traffic that conforms to these rules can be allowed, while unexpected traffic inspected for potential instrusions. Such an approach dramatically reduces load on the IDS, allowing it to scale in performance and identify device-specific threats.

- Ayyoob Hamza, et al. Combining MUD Policies with SDN for IoT Intrusion Detection. IOT S&P.

To address the above problems, we propose Pagoda, a provenance based intrusion detection system that analyzes the anomaly degree of not only a single path, but also the entire provenance graph. It first looks for the intrusion path that may result in the intrusion. If the path has been found, then it does not have to traverse the provenance graph for further detection. Otherwise, it computes the anomaly degree of the provenance graph in three steps.

Moreover, like many provenance systems (e.g., CamFlow [21]), Pagoda filters unnecessary provenance data to reduce the detection time. This also prevents noisy data generating false alarms. Typical noisy data includes daemon processes, pipe files and temporary files that are not likely to contain intrusion information. As Pagoda mainly uses the dependency relationships between different objects to drive the intrusion detection algorithm, it also omits some provenance data (e.g., environment variables and input parameters) to save the memory space. In addition, as we use an absolute path name to describe a file or a process, files in the same directory have a common prefix in their names. Pagoda uses dictionary encoding [22] technology to compress these duplicates to further reduce the space overhead.

- Yulai Xie, et al. Pagoda: A Hybrid Approach to Enable Efficient Real-Time Provenance Based Intrusion Detection in Big Data Environments. IEEE Transactions on Dependable and Secure Computing.

---

(2) 贡献总结经典句子

> **常用的本文贡献引入句子：**
>
> - In summary, MAGPIE implements the following contributions:
> - The contributions of our paper are summarized as follows:
> - In summary, the contributions of this paper are as follows:

> - The main contributions of this work are summarised as follows:
> - In summary, the contributions of our paper are five-fold:
> - The main contributions are summarized as follows:
> - In summary, we make the following contributions:
> - The contributions of this paper are as follows:

We present Whisper, a novel malicious traffic detection system by utilizing frequency domain analysis, which is the first system built upon machine learning achieving realtime and robust detection in high throughput networks.

We perform frequency domain feature analysis to extract the sequential information of traffic, which lays the foundation for the detection accuracy, robustness, and high throughput of Whisper.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

We systematically investigate practical AE attacks and defenses of recent ML-based IDSs. To the best of our knowledge, we are the first to investigate AE attacks for IDS in problem space rather than in feature space, and also the first to propose an effective AE detection scheme to defend against such attacks.

We propose MANDA, a novel MANifold and Decision boundary-based AE detection scheme for ML-based IDS. MANDA is designed by exploiting unique features we observe while trying to categorizing AE attacks from the viewpoint of machine learning model and data manifold. Based on our AE categorization, MANDA combines two building blocks (i.e., Manifold and DB) together to achieve effective AE detection regardless of which AE attack is used.

Our experimental results show that MANDA achieves 98.41% true-positive rate (TPR) with a fixed 5% false-positive rate (FPR) under CW attack, the most powerful AE attack, and over 0.97 AUC-ROC under three frequently-used attacks (FGSM attack, BIM attack, and CW attack) on the NSL-KDD dataset. We also demonstrate that MANDA outperforms Artifact [17], a state-of-the-art solution on AE detector, on both IDS task and image classification task.

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

We improve the ensemble learning model in the model training stage, based on our finding that different detection algorithms have different sensitivities to different attacks. The

individual classifier adaptively selects different weights for different attack types according to their classification confidence and the output probability, thereby improving the detection accuracy of the model. And multi-class regression models are trained to fuse individual classifiers' results.

In the model update stage, we design a model knowledge transmission method based on incremental learning. The parameters of historical models are transmitted to the new model for pre-training, and the detection results of the historical model are added to the training process of the new model. In this way, the sustainability of the model update is maintained, and the false alarm and false negative rates are reduced. As far as we know, we are the first to reuse of knowledge in the historical detection model in the IDS system.

- Xinghua Li, et al. Sustainable Ensemble Learning Driving Intrusion Detection Model. TDSC.

Ability to continuously adapt unsupervised smart home threat detection to changing conditions. MAGPIE self-adapts by applying reinforcement learning on the unsupervised classifier's hyperparameters based on a probabilistic reward function without an a priori model or knowledge of the household configuration.

Experimental evaluation with both cyber and physical sources of data. From a threat monitoring perspective, the physical impact of some security breaches constitutes an opportunity because, in conjunction with traditional cyber sources of data, it can provide valuable information about the system's security state.

- Ryan Heartfield, et al. Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. IEEE TIFS.

This work proposes a new filter-based feature selection method, in which theoretical analysis of mutual information (MI) is introduced to evaluate the dependence between features and output classes. The most relevant features are retained and used to construct classifiers for respective classes. As an enhancement of Mutual Information Feature Selection (MIFS) [11] and Modified Mutual Information-based Feature Selection (MMIFS) [12], the proposed feature selection method does not have any free parameter, such as b in MIFS and MMIFS. Therefore, its performance is free from being influenced by any inappropriate assignment of value to a free parameter and can be guaranteed. Moreover, the proposed method is feasible to work in various domains, and more efficient in comparison with HFSA [10], where the computationally expensive wrapper-based feature selection mechanism is used.

- Mohammed A. Ambusaidi, et al. Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. IEEE TRANSACTIONS ON COMPUTERS

Different from the detection framework proposed in [10] that designs only for binary classification, we design our proposed framework to consider multi-class classification problems. This is to show the effectiveness and the feasibility of the proposed method.

- Mohammed A. Ambusaidi, et al. Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. IEEE TRANSACTIONS ON COMPUTERS

We present WATSON, the first approach to abstracting high-level behaviors from low-level logs without analyst involvement. Our approach summarizes behaviors using information flow as guidance and derives behavior semantics by aggregating contextual semantics of audit events.

We propose the novel idea of inferring log semantics through contextual information. We provide a quantitative representation of behavior semantics and use it to cluster semantically similar behaviors and extract representatives.

We prototype WATSON and conduct a systematic evaluation with both commonly-used benign behaviors and real-world malicious behaviors. The results show that WATSON is effective in abstracting high-level behaviors and reducing human workload in the analysis of logs.

- Jun Zeng, et al. WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics. NDSS.

We devise a disagreement-based semi-supervised learning algorithm, which can leverage the unlabeled data for classification, and investigate its use in the field of intrusion detection. In addition, we develop a framework of DAS-CIDS by applying the disagreement-based semi-supervised learning to improve the performance of CIDSs, in the aspects of detection performance and alarm filtration.

In the evaluation, we perform two major experiments to exploit the performance of our approach with real datasets and in a real IoT environment, respectively. Our results indicate that the disagreement-based method can outperform traditional supervised machine learning classifiers by learning from unlabeled data, during anomaly detection and alarm filtration.

- Wenjuan Li, et al. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. Journal of Network and Computer Applications.

We propose Pagoda, a provenance-based intrusion detection system that takes into account the anomaly degree of both a single path and the whole provenance graph to achieve both fast and accurate detection in big data environments.

To further save the memory space, we apply dictionary encoding to reduce the replicated items in the rule database. Moreover, we filter the noise provenance that is not likely to contain intrusion information or is not used for detecting intrusions in our method. Thus we improve the detection accuracy and reduce the detection time.

We implement the system prototype and evaluate it on a series of real-world normal and vulnerable applications. The experimental results show that Pagoda significantly outperforms the classical syscall-based method [5] and the state-of-the-art (i.e., provenance path based method [17]) on a series of critical axes, such as detection accuracy, detection time, forensic analysis efficiency and space overhead.

- Yulai Xie, et al. Pagoda: A Hybrid Approach to Enable Efficient Real-Time Provenance Based Intrusion Detection in Big Data Environments. IEEE Transactions on Dependable and Secure Computing.

We proposed a few-shot network intrusion detection method based on a meta-learning framework. This method can be used to learn prior knowledge for network traffic classification directly from original traffic. After obtaining sufficient prior knowledge, new types of traffic can be detected with a few-shot of samples.

We proposed a method to construct datasets to perform training corresponding to few-shot network intrusion detection based on real network traffic. Using this method, we constructed two datasets incorporating the data public network traffic data sources and conducted two types of experiments on these datasets.

We demonstrated that the proposed network intrusion detection method is universal and is not limited to specific attack types. Using the proposed method, new types of samples on the basis of only a limited number of labels in an untrained dataset can be detected relying on learned prior knowledge.

- Congyuan Xu, et al. A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework. IEEE Transactions on Information Forensics and Security.

综述类：

We systematically review existing deep learning-based anomaly detection methods that target at detecting faults and attacks in CPS. To this end, we propose a new taxonomy that is based on (i) type of anomalies (i.e., threat model), (ii) detection strategies (i.e., input data, neural network designs, anomaly scores), and (iii) implementation and evaluation metrics. Further, we explore and categorize peer reviewed research papers from conferences and journals under the setting of this taxonomy.

We identify and highlight characteristics that are essential to building a DLAD method. First, we discuss existing methods in representative CPS domains (i.e., ICSs, smart grid, ITSs, and aerial systems). Then, we report unique designs and trends in each domain. All these findings are summarized according to our taxonomy. Meanwhile, we summarize and discuss the limitations and open problems of current methods.

We identify the limitations and deficiencies of deep learning approaches when being applied to the anomaly detection task in CPS. We present our findings and takeaways to improve the design and evaluation of DLAD methods. Also, we discuss several promising research directions and open problems that motivate future research efforts.

- Yuan LUO, et al. Deep Learning-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities. ACM Computing Surveys.

第5部分：工作安排

该部分可省略，建议结合作者习惯撰写。

The rest of the paper is organized as follows: Section 2 introduces the threat model and the design goals of Whisper. Section 3 presents the high-level design of Whisper. In Section 4, we present the design details of Whisper. In Section 5, we conduct a theoretical analysis. In Section 6, we experimentally evaluate the performances of Whisper. Section 7 reviews related works and Section 8 concludes this paper.

- Chuanpu Fu, et al. Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis. CCS.

The remainder of this article is organized as follows. Section II presents the problem formulation and logic flow of this article, and Section III introduces the second order NPGF-based sensor data reconstruction model and its frequency-domain analysis method. In Section IV, the error function concerning the artificial perturbations is derived in the frequency domain, and a detection algorithm is developed based on the high-frequency components. Numerical studies and discussions are presented in Section V, and finally, Section VI concludes this article.

- Zhenlong Xiao, et al. Anomalous IoT Sensor Data Detection: An Efficient Approach Enabled by Nonlinear Frequency-Domain Graph Analysis. IOTJ

The rest of this article is organized as follows. We briefly summarize related work in Section 2, and introduce the basic methods and architecture of our model in Section 3, and present the proposed intrusion detection model in detail in Section 4, and the corresponding experimental analysis is given

in Section 5. Finally, Section 6 concludes our work.

- Xinghua Li, et al. Sustainable Ensemble Learning Driving Intrusion Detection Model. TDSC.

The rest of the paper is organized as follows. § 2 presents the motivation of this work. § 3 gives an overview of vNIDS architecture. § 4 discusses the state management approaches to ensure the detection effectiveness as well as minimizing the performance overhead. § 5 presents how to decouple monolithic NIDS into microservices to achieve the efficient provisioning. Implementation and evaluation of vNIDS are presented in § 6 and § 7, respectively. Discussion and related work are addressed in § 8 and § 9, respectively. Finally, we conclude in § 10.

- Hongda Li, et al. vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems. CCS.

The remainder of the paper is organized as follows. Section II summarizes the related work. Section III introduces the system model and threat model. In Section IV, we elaborate the proposed AE detection scheme. We then present and compare the experimental results in Section V. Conclusion are drawn in Section VI.

- Ning Wang, et al. MANDA: On Adversarial Example Detection for Network Intrusion Detection System. IEEE INFOCOM 2021

三.总结

这篇文章就写到这里了，希望对您有所帮助。由于作者英语实在太差，论文的水平也很低，写得不好的地方还请海涵和批评。同时，也欢迎大家讨论，真心推荐原文。学安全两年，认识了很多安全大佬和朋友，希望大家一起进步。同时非常感谢参考文献中的大佬们，感谢老师、实验室小伙伴们的教导和交流，深知自己很菜，得努力前行。感恩遇见，且行且珍惜，小珞珞太可爱了，哈哈。

谢谢CSDN的实体勋章和无线耳机，很幸运，1024写文混了第一名（因为有小珞）希望今年能写上120篇原创文章，在这么忙碌的博士生涯，能写这些真心不容易，都是挤出来的。

最后感谢CSDN和读者们十年的陪伴，不论外面如何评价CSDN，这里始终是我的家，在这里写文章很温馨，也认识了很多大佬和朋友。此外，个人感觉今年是我近十年文章质量最高的一年，每一篇都写得很用心，都是我的血肉，很多都要自己从零去学习再分享，也希望帮助更多初学者。总之，希望自己还能写二十年，五十年，一辈子。这些年CSDN改进真挺多的，也一直为博主着想，希望越来越好。感恩同行，一起加油喔，以后没准小珞珞接管“Eastmount”这个账号，哈哈！

(By:Eastmount 2021-11-23 晚上12点 http://blog.csdn.net/eastmount/)

文章知识点与官方知识档案匹配，可进一步学习相关知识