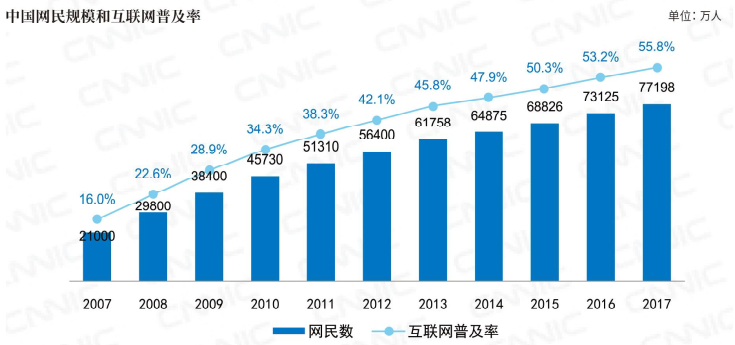
## 研究背景与意义

随着计算机技术和网络通信技术的不断发展以及在政治、经济、军事等领域的日益普及和广泛使用，互联网已成为全社会信息交流和共享的重要媒介，是人们生活、工作、学习和娱乐中不可或缺的重要部分。

2018年1月31日，中国互联网信息中心在北京发布了《中国互联网络发展状况统计报告》[[[1]](#endnote-0)]。报告指出截 至2017年12月，我国网民规模达7.72亿，同1997年10月第一次调查结果62万网民人数相比，现在的网民人数已是当初的1245.2倍。2017年全年共计新增网民4074万人，互联网普及率为55.8%，较2016年底提升2.6个百分点。从下图可以看出我国网民规模和互联网普及率逐年增长，短期内还会持续上升的的趋势。



互联网技术广泛普及的同时，也带来了一系列信息安全事件，信息安全事件每年层出不穷，给国家，企业和个人带来了巨大的经济损失。根据2010年度信息安全报告[[[2]](#endnote-1)]统计，各种类型病毒增长迅速，网络攻击、网络病毒已成为危害网络安全的主要因素。

2000年2月，美国的Yahoo、CNN、Amazon等多家著名商业网站遭受到历史上最大规模的分布式拒绝服务攻击（Distributed Denial of Service，DDOS），黑客使用多台计算机发送大量电子请求来阻塞服务器，使这些网站一度陷入瘫痪，据统计，这次攻击事件导致的经济损失高达10亿美元以上。2002年10月，管理全球互联网运作的13台根域名服务器遭受分布式拒绝服务攻击，其中9台一度因此终止服务。

2017年5月，一种“蠕虫式”的勒索病毒案软件，由不发分子利用NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”进行传播，100过个国家和地区超过10万台主机遭到攻击、感染，至少150个国家、30万名用户中招，造成经济损失达80亿美元，影响到警容，能源，医疗等众多行业，造成严重的危机管理问题。 中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。该病毒已经是一个军事级别的病毒了，完全可以在互联网战争中摧城拔寨。而这场“互联网瘟疫”已经是一次使用军事级别技术针对平民的无差别攻击了，相当于一次全球范围恐袭。2017年7月，美国征信企业Equifax对外宣布，因公司网站遭到黑客攻击，1.43亿美国公民的信息数据或已被泄露。此次泄露的内容包括个人的姓名、住址、出生日期、社会安全号码等信息。除此以外，此次泄露的数据还包括20.9万人的信用卡卡号、18.2万人的特定争议文件等。

俄罗斯央行遭黑客攻击，3100万美元不翼而飞，黑客通过伪造证书入侵；雅虎5亿用户信息被黑客盗取，盗取内容包括用户的姓名、电邮地址、电话号码、生日、密码等，甚至还包括加密或未加密的安全问题及答案；全球第二大社交网站MySpace 3.6亿的用户账号以及4.27亿的密码被黑客获取并在暗网上以2800美元的价格销售这批数据。

由此可见，信息安全事件日益增加，新的攻击手段层出不穷，给政治、经济、军事等领域大带来了严重的威胁和巨大的损失，如何保证信息系统的安全运行成为不可忽视的问题，这具体体现为[[[3]](#endnote-2)]：

1. 互联网技术的发展使得计算机系统遭受入侵的风险性急剧增加。互联网改变了过去以单机为主的计算模式，计算机在资源共享及分布系统等方面的计算能力得到空前提高，这也给黑客攻击和入侵提供了物质基础，黑客可以远程攻击目标系统。过去几年，黑客攻击的数量快速增长，攻击对象包括了所有接入网络的计算机系统，如政府、军方、商业及个人计算机系统，攻击目的有占用系统服务资源，典型的如DoS攻击、篡改数据和盗取机密数据等。
2. 互联网技术给计算机病毒提供了新的途径。计算机病毒已从最初的磁盘介质为载体的传播方式发展为以电子邮件、软件下载为手段的网络传播方式，传播速度和传播范围都急剧增大，计算机病毒已成为计算机系统和网络发展的巨大危害。
3. 信息系统，特别是软件系统的复杂化伴孕育着越来越多的安全漏洞，严重威胁了信息系统的安全。同控制系统一样，软件系统越复杂其正确性越难以保证，越容易出现漏洞。近年来，随着人民对互联网的依赖越来越强，软件系统的功能越来越强大，代码量越来越多，例如微软的操作系统从当初DOS的数千行代码发展到现在Windows10的接近1亿的代码量，这使得漏洞出现的几率越来越大。
4. 移动互联网。依托于移动互联网的终端设备，例如手机、平板等已经成为大部分人生活中不可或缺的部分。截止2017年12月，我国手机网民规模达7.53亿，较2016年底增加了5734万人，网民中使用手机上网人群的占比由2016年的95.1%提升至97.5%，网民手机上网比例继续攀升。这给不法分子提供了更好的入侵平台，例如利用手机恶意代码窃取用户隐私信息、恶意定购各类增值服务。手机恶意代码增长速度快、传播范围广、危害大，移动互联网网络环境治理工作亟待加强。

随着入侵手段不断的更新和入侵规模逐渐增大以及网络上提供多种现成的黑客工具，传统的信息安全技术（机密，身份认证和访问控制）在这些复杂的攻击面前显得极为脆弱，漏洞逐渐被暴露出来，例如访问控制通过设定主体对执行访问行为的对象的访问管理，可以在一定程度上保证安全，但是如果需要追求更高的安全性，则需要实现细粒度的访问控制技术，做到权限管理力度的最小化，然而这样做会带来很多的实际问题，如系统权限管理效率低下、管理员权限管理难度增大等，从而使权限滥用的问题不能很好地得到解决。身份认证是通过鉴别访问者的身份来实施授权，但是研究表明，由于漏洞的存在和社会工程学的作用，存在大量绕过身份认证的非法访问。数据加密技术，只能做到信息的机密性，不能保证完整性和可用性。正式由于传统的安全技术存在这样或那样的不足，入侵检测技术得以全面发展。

入侵检测技术作为一种主动防御技术，通过对主机系统和网络的实时监控，一旦发现可疑的入侵事件，就会采取相应的措施（如通知管理员，切断网络连接等），因此能够有效的解决以身份认证和访问控制为核心的传统安全技术难以解决的安全问题。传统安全技术相对固定，一旦被突破，系统将毫无办法。入侵检测系统（Intrusion Detection System，IDS）被认为是防火墙之后的第二道安全屏障，是信息安全技术的重要组成部分，日益受到各国政府的关注和重视，目前，针对入侵检测技术的研究已成热点，同时，许多商用的入侵检测系统已经投入使用，但是由于互联网的开放性、移动性以及网络系统的日趋复杂性，使得入侵检测系统的性能（检测准确率、漏报率和误报率）仍有待提高。

## 计算机网络安全和入侵检测

### 计算机网络安全

广义的计算机安全定义[[[4]](#endnote-3)]是：主体的行为完全符合系统的期望，系统的期望表达成安全规则，也就是说主体的行为必须符合安全规则对它的要求。

根据OSI的狭义的系统与数据安全性定义[[[5]](#endnote-4)]：

* 机密性(confidentiality)：使信息不泄露给非授权实体，包括个人和进程等，不被其所利用。
* 完整性(integrity)：数据没有遭受以越权方式所作的篡改或破坏。
* 可确认性(accountability)：当计算机遭受攻击后，安全系统有充足的信息追踪和识别入侵者。
* 可用性(availability)：授权实体可以访问和使用。

上诉计算机安全的各项特性取决于计算机系统安全策略的需求，这些安全策略用来定义或描述系统的不同用户和软件模块的行为，并明确指出哪些行为是合法的，哪些是被禁止的。

随着互联网和云技术的高速发展，网络安全的概念也被提出。相比较于计算机安全，网络安全在保证网络资源的机密性、完整性、可确认性和可用性的同时，还存在更加复杂的安全问题，如资源的共享、网络拓扑结构的多样性、未知的边界、不同操作系统之间的安全通信等[[[6]](#endnote-5)]。网络安全问题正得到越来越多的人的关注和重视，然而网络入侵事件的数量却逐年攀升。现代黑客从以系统为主的攻击转为以网络为主的攻击[[[7]](#endnote-6)]，攻击手段变得越来越丰富，如网络监听、端口扫描、拒绝服务、利用匿名用户访问攻击、越权操作以及通过秘密通道绕过防火墙的攻击方法等。

### 入侵检测

入侵检测[[[8]](#endnote-7)]是近年来发展起来的一种动态监测、预防或抵御系统入侵行为的安全机制。通过收集和分析[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C)行为、[安全日志](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E6%97%A5%E5%BF%97)、审计数据、其它[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C)上可以获得的[信息](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF)以及[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F)中若干关键点的信息，它能够检查网络或系统中是否存在违反[安全策略](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E7%AD%96%E7%95%A5)的行为和被攻击的迹象，从而发现并处理相应的安全事件。入侵检测通过以下行为达到检测目的：监视、分析用户及系统活动，系统构造和弱点的审计，识别反映已知攻击的活动模式并向相关人士报警，异常行为模式的统计分析，评估重要系统和数据文件的完整性，操作系统的审计跟踪管理，并识别用户违反安全策略的行为。区别于防火墙，入侵检测用来发现已经发生的入侵事件，然后把结果报告给相关责任人，而防火墙限制了主机在网络间的通信从而防止入侵发生。

入侵检测技术根据不同的侧重点从而有不同的分类方法。根据审计数据来源和所监控的对象的不同，可以分为基于主机的入侵检测系统（Host based intrusion detection system，HIDS）、基于网络的入侵检测系统（Network based intrusion detection system，NIDS）和混合分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）。基于网络的入侵检测主要侧重于网络传输数据流内容检测、远程节点检测与控制等方面；基于主机的入侵检测主要侧重于检测进程的运行状态、磁盘存储资源和网络链接状态等方面[[[9]](#endnote-8)]；根据反应机制的不同，可以分为主动型入侵检测和被动型入侵检测；按照检测方法的不同，可以分为误用检测（Misuse Detection）和异常检测（Anomaly Detection）[[[10]](#endnote-9)]。

基于网络的入侵检测技术侧重于分析所有经过被监控网段的流量，对获取的流量进行分析处理，从中提取有用的信息，再通过与已知攻击特征相匹配或与正常网络行为原型相比较来识别攻击事件。此类检测技术不再依赖操作系统作为检测资源，可应用于不同的操作系统平台；配置简单，不需要任何特殊的审计和登录机制；可检测协议攻击、特定环境的攻击等多种攻击。但它只能监视经过本网段的活动，无法得到主机系统的实时状态，精确度较差。大部分入侵检测工具都是基于网络的入侵检测系统。

基于主机的入侵检测技术仅仅使用在单一主机上，该类检测技术包括分析所有进出该主机的流量和主机系统关键文件的对比等，它一般使用操作系统的审计、跟踪日志作为数据源。该类技术优点是对网络流量不敏感，检测效率高，能准确定位入侵并及时进行反应，缺点是占用主机资源，检测攻击类型有限，不能检测网络攻击。

混合分布式入侵检测系统采用分布式结构，由多个部件构成，其核心机制是在关键主机上采用基于主机的入侵检测，在网络关键节点上采用网络入侵检测，同时分析来自主机系统的审计日志和来自网络的数据流，判断被保护系统是否受到攻击。

误用检测也叫基于特征的检测技术，首先要定义违背安全策略的事件的特征，如网络数据包的某些元信息，通过匹配发现是否出现对应的攻击，常见的方法有模式匹配，专家系统等。异常检测首先建立系统的正常运行模式，可从以下几个方面建立运行模式：CPU利用率、内存利用率和系统关键文件校验和等，然后根据主机或者网络的行为与正常运行模式的偏离来检测异常，若与正常运行模式相差较大，超过预定义的阈值，则可以判定系统或者网络正在遭受攻击。误用检测具有滞后性，特征库需要不断维护更新，对于已知的攻击，它可以详细准确地报告出攻击类型，检测率高，但是对于新的攻击手段却效果有限，甚至根本无法识别。基于异常的检测技术无法准确地判断攻击的手段，但是它对新的攻击类型敏感，理论上，它可以判别更广泛，甚至最新的攻击手段。异常入侵检测的理想状态是，异常行为等同于入侵行为，但是在实际中这难以达到，异常检测将所有不符合既定系统状态的行为产生报警，因此误报率较高[[[11]](#endnote-10)]。

### 入侵检测技术评价指标

评价一个入侵检测技术优劣的指标有很多，本文选取最重要的三个指标作为后续实验结果的评价依据，包括分类正确率、漏报率和误报率。

1. 分类正确率指的是被正确归类的样本总数和全体测试样本总数的比值，描述算法的分类效果，该值越高，算法总体的检测能力越强，我们希望分类正确率越高越好。
2. 误报率是指被错误归类为攻击样本的正常样本数和全体测试样本总数的比值，误报率越低，算法对于正常样本的识别能力越强，算法效果越好。
3. 漏报率是指被归类为正常样本的攻击样本个数和全体测试样本总数的比值，这个值反应了入侵检测技术对于攻击的识别能力，如果测试样本中含有大量在训练样本中没有出现的攻击类型，则这个指标也可以从一定程度上反应对未知攻击的识别能力，漏报率越低，算法效果越好。

## 国内外研究现状

早在20世纪80年代就已经展开了对入侵检测技术的研究，发展至今已有近30年的历程。

1980年，Anderson J P提出了入侵检测的基本概念[[[12]](#endnote-11)]。他将入侵尝试（Intrusion Attempt）或威胁（Threat）定义为：在未经授权的情况下访问信息、操作信息，致使系统不可靠或不可用的企图。同时他提出了以操作系统审计数据为依据进行入侵检测的思想，迫于当时的信息安全措施都着重于加密和拒绝未经认证主体对重要数据的访问，这一思想并未引起人们的重视。

1987年Dorothy Denning博士提出了入侵检测系统的抽象模型[[[13]](#endnote-12)] ，该模型被称为“入侵检测专家系统（Intrusion Detection Expert System，IDES）”，它由主体（Subjects）、对象（Objects）、审计记录（Audit Records）、轮廓特征（Profiles）、异常记录（Anomaly Records）、活动规则（Activity Rules）等六部分组成，该文献首次将入侵检测的概念作为一种计算机系统安全防御问题的措施提出，是入侵检测早期研究中最重要的成就之一，在入侵检测技术的发展历史中具有里程碑式的意义。相比较于传统加密和访问控制的常用方法方相比，IDS是全新的计算机安全措施。

1988年，Teresa L等人对Dorothy Denning提出的模型进行了改进，提出了与系统平台无关的实时检测思想，并创建了实际的IDES，该系统最初用于检测针对单一主机的入侵行为。1995年开发了IDES完善后的版本-NIDS（Next-Generation Intrusion Detection System），支持在多个主机上检测入侵。1988年，美国空军开发了Haystack系统[[[14]](#endnote-13)]，同年，出现了为美国国家计算机安全中心Multics主机开发的MIDAS（Multics Intrusion Detection and Alerting System）[[[15]](#endnote-14)]，1989年，Los Alamos 美国国家实验室开发了W&S（Wisdom and Sence）系统[[[16]](#endnote-15)]，Planning Research公司开发了ISOA（Information Security Officers’ Assistant）[[[17]](#endnote-16)]。

1980年到1990年间是入侵检测系统从无到有的奠基时期，这一阶段的提出了入侵检测的概念和基本模型，实现了简单的IDS系统。从之前的研究可知，该时期的IDS都是针对单一主机的，检测数据来源都是主机系统的待审计数据。然而随着互联网的普及和高速发展，针对网络的攻击事件层出不穷，数量不断攀升，对入侵检测的研究也因此进入了一个新的阶段，即网络入侵检测技术。

1990年，Heberlein L T提出了“基于网络的入侵检测”的概念[[[18]](#endnote-17)]，描述了基于网络的入侵检测系统-NSM（Network Security Monitor），该系统数据来源并不是主机的审计记录和日志等，而是通过在共享网段上对数据包进行监听和采集，分析包头信息，尽量找出可能出现的攻击事件，从而保护整个网段免受入侵，该方法扩展了入侵检测技术的应用范围，同时由于采用监听方式来获取数据，因此不会增加网络负担，更不会占用网段上其他主机的资源。这标志了NIDS时代的来临。

1991年，NADIR（Network Anomaly Detection and Intrusion Reporter）[[[19]](#endnote-18)]与DIDS（Distribute Intrusion Detection System）[[[20]](#endnote-19)]提出了收集和合并处理来自多个主机的审计信息，用来检测针对一系列主机的协同攻击。这是入侵检测发展史的第一个分布式系统，它将主机入侵检测和网络入侵检测相结合，能够适应异构环境，对分布式入侵检测技术的研究也掀开了篇章。

1994年，Mark Crosbie和Gene Spafford建议使用自治代理（Autonomous Agents），其目的是为了提高IDS的可伸缩性、可维护性、效率和容错性，这一理念非常符合正在进行的计算机科学其他领域如软件代理的研究[[[21]](#endnote-20)]。

1996年，GRIDS（Graph-based Intrusion Detection System）的设计和实现是为了解决当时绝大多数入侵检测系统伸缩性不足的缺点，该系统使对大规模自动或协同攻击的检测变得更为便利，这些攻击有时甚至可能跨过多个管理领域。同年，Forrest等人将免疫原理运用到分布式入侵检测领域并取得了不错的效果；1998年Ross Anderson和AKhattak给入侵检测带来了创新-信息检索技术被引进到入侵检测[[[22]](#endnote-21)]；Lane T等人对基于机器学习的用户行为异常检测进行了研究；Lee W等人将数据挖掘技术应用于入侵检测[[[23]](#endnote-22)]；Warrender C等人以系统调用为审计数据，进行了基于隐马尔科夫模型的程序行为异常检测研究[[[24]](#endnote-23)]。

2000年2月，对美国多家著名互联网公司（Yahoo、Amazon、CNN等）的DDOS攻击引发了对入侵检测的新一轮研究热潮，研究方向扩展到了全面地检测攻击行为，包括网络、主机和分布式等攻击方式。

与防火墙、加密、认证等成熟的网络安全技术相比，目前的入侵检测技术还存在较大的改进空间，其缺陷主要是检测正确率比较低，实时性差，自学习能力不强，而且当前真正投入市场的IDS几乎都是基于模式匹配的误用检测方法，如上讨论，这种检测技术对于新攻击毫无办法，而且系统的攻击规则库需要不断的、快速的补充和更新，这使得维护成本急剧增大。

目前，入侵检测技术的研究主要集中的美国，而且许多的研究成果都直接或者间接地得到了美国政府和美国军方的支持，并且在许多领域得到了应用[[[25]](#endnote-24)]。美国政府或军方参与的入侵检测技术研究的高校主要有普渡（Purdue）大学、麻省理工学院（Massachusetts Institute of Technology）、新墨西哥（New Mexico）大学和加利福尼亚（California）大学等，与此同时，一些公司也参与到入侵检测技术的研究和实现，这其中比较出名的是美国敏源国际（ISS）有限公司开发的RealSecure系统、Cisco公司开发的NetRanger入侵检测系统、Axent公司开发的NetProwler系统以及CyberSafe公司开发的Centrax系统等，实践表明，这些系统具有比较完善的功能和较强的实用性。相较于西方国家，国内在入侵检测这块则起步比较晚，大部分的研究只是跟踪、模仿国外的技术。近几年，鉴于互联网的高速发展和信息安全变得刻不容缓，我国对入侵检测的研究经费投入也在不断增加，目前一些涉及入侵检测的“国家自然科学基金”项目和“863”项目正在开展，并取得了一些可喜的结果。国防科技大学、清华大学、中国科学院、中南大学、西安电子科技大学、南京大学、浙江大学等单位都在进行相关研究。但是总体而言，国内自行研制的入侵检测系统相对较少，功能比较简单和单一，因此在研究入侵检测技术这块我们应该继续加大投入更多的物力和人力。

今后入侵检测技术将主要向分布式、智能化、云计算环境、高检测速度、高准确度、高安全性的方向发展，研究重点将会包括以下几个：

1. 分布式入侵检测。随着云计算的高速发展，网络计算机的概念被提出，它主要采用分布式结构，用于解决单一主机无法满足人们日益增加的网络性能要求。当前的许多服务器都采用分布式结构，因为分布式入侵检测系统的需求将逐步攀升，针对分布式系统的入侵检测研究也将迫在眉睫。
2. 智能入侵检测。智能入侵检测技术是将入侵检测和人工智能相结合，包括机器学习、神经网络、数据挖掘等方法。智能检测是异常检测的扩展，主要是解决误用检测无法识别新型攻击手段等缺点，同时提高分类正确率和降低误报率和漏报率。
3. 基于协议分析的入侵检测。对网络型入侵检测系统而言，如果其检测速度跟不上网络数据的传输速度，检测系统就会漏掉其中的部分数据包，从而导致漏报而影响系统的准确性和有效性。大部分现有的网络型入侵检测系统只有几十兆的检测速度；目前，百兆甚至千兆网络的大量应用，对系统的检测速度提出了更高的要求。基于协议分析的呃呃入侵检测所需的计算量相对较少，可以利用网络协议的高度规则性快速探测攻击的存在，即使在高负载的网络上也不容易产生丢包现象。
4. 结合操作系统。目前入侵检测系统的普遍缺陷是与操作系统结合不紧，导致很多不便，例如很难确定黑客攻击系统到了什么程度，不知道黑客拥有了系统那个级别的权限，黑客是否控制了一个系统等。与操作系统的紧密结合可以提升入侵检测对攻击，特别是比较隐蔽的、新出现的攻击的检测能力。
5. 融合多种入侵检测技术。当前的许多IDS只采用单一的入侵检测技术，随着互联网技术的高速发展，服务器系统的架构将会变得越来越复杂，单一的入侵检测技术将无法很好地检测到对这些复杂系统的攻击。将误用检测和异常检测结合起来构造IDS将是很好的解决方案，有助于提高检测正确率，降低误报率和漏报率。

应用层入侵检测、高速报文捕获技术、高效的模式匹配算法、入侵检测系统的测试和评估、入侵检测系统的标准化、入侵检测系统之间以及入侵检测系统和其它安全组件之间的互动性研究和入侵检测系统自身安全性的研究也是未来在入侵检测这块研究的重点和热点。

# 数据集和特征提取

## 3.1 数据集简介

### 3.1.1 数据集来源

KDD CUP99数据集[[[26]](#endnote-25)]是经典的入侵检测数据集，是大部分研究人员用于训练和测试入侵检测模型的Benchmak。此数据集是1999年KDD竞赛所使用的数据集。该数据集是由麻省理工学院林肯实验室主持，通过美国国防高级规划署（DAPRA）搭建的局域网网络环境，利用Linux中常用的网络抓包工具，统计了9个星期的所获得的详细的Raw TCPDUMP格式的网络数据，其中训练集包括500万条连接的数据，测试集包括200万条连接的数据，所有连接都是基于TCP协议的，每个连接被标记称正常或者异常。该环境能够较真实的模拟用户的网络行为（其中模拟了政府和军队的1000个主机上的100多个用户），获取比较全面的网络数据。

该数据集主要由以下几个部分构成[[[27]](#endnote-26)]：

1. 含有所有数据的集合：kddcup.data.gz（可用于实验训练阶段）；kddcup.testdata.unlabeled.gz（可用于实验测试阶段）；
2. 部分数据集：kddcup.data\_10\_percent.gz（占全部训练数据集的10%，已注明攻击类型）；kddcup.newtestdata.unlaeled\_10\_percent.gz（占全部测试数据集的10%，未注明攻击类型）；
3. Corrected.gz，此文件为上一部分中未注明攻击类型的数据，提供攻击类型标注，通常在仿真实验中使用该部分数据集对实验结果进行分析和比较。

通过阅读大量文献，我们发现，研究人员大多使用10%数据集，用其训练数据集对神经网络模型进行训练，用测试数据集对研究结果进行测试，最后用corrected数据集对使用测试数据集检测的实验结果进行比较和分析。

### 3.1.2 数据集内容构造分析

在KDD CUP99提供的10%数据集中，总共有38种攻击类型，这38中攻击类型又可以分为4大特征较明显的攻击类型：

1. Denial-Of-Service（DOS）:是指入侵者使用正常的手段发送大量无效请求，从而占用了服务器大部分资源，使合法用户的正常服务来不及或根本无法得到响应，造成服务瘫痪现象，是比较常见的入侵手段之一，如SYN洪水攻击等；
2. Surveillance or Probe：对计算机系统的漏洞进行探测，例如进行端口扫描、猜测口令或者ping地址等方式；
3. User to Root（U2R）：指通过向目标主机发送网络数据包的方式试探本地访问权限的入侵方式；
4. Remote to Local（R2L）：是指入侵者利用目标系统的漏洞，使用普通权限用户登录后，获取系统级权限的行为。

从细分攻击类型的角度上分析，在10%的训练数据集和10%的测试数据集中，所包含的攻击类型数量并不相同。训练集中共有23种入侵类型，测试集中包含所有的38种入侵类型，其中15种新攻击类型未在训练集出现，训练集和测试集的数据分布如表3-1和表3-2所示：

表3-1 KDD CUP99数据集的攻击分类

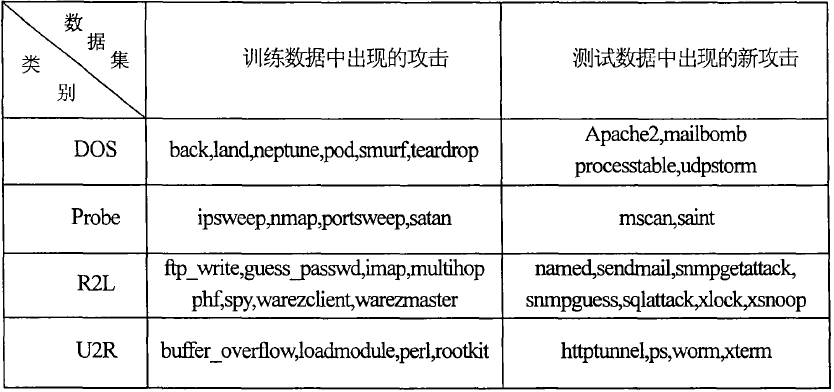


表3-2 入侵数据分布



Wenke Leee建立了KDDCUP’99项目，从大量冗余信息的数据中提取了较多的有用安全数据和有利于进行判断和比较的特征集合。Lee从DARPA1998数据中抽取了41维特征，分为基本特征（basic features）、内容特征（content features）、两秒钟内的流量特征（traffic features computed using a two-second time window）、主机流量特征（host-based traffic features）。考虑到有部分特征项含有无数值意义的字符项，为了便于我们的模型处理，对其进行了数值混合编码，即将具有数值意义与不具有数值意义的信息按数值形式统一进行编码的方式。如包含有无数值意义的服务类型（Service），和有数值意义的从源到目的比特数Src\_bytes。

3.1.2.1 基本特征（basic features）

基本特征反应了一个独立连接的基本属性，有以下特征：

1. duration：连续持续时间
2. protocol\_type：连接使用的协议，我们以IP协议中的协议类型进行编码，TCP=6、ICMP=1、UDP=17。
3. service：服务类型。如ftp、http、telnet、time等，按照服务常用端口号进行编码。
4. flag：连接终止状态。flag有11个状态。我们对其进行编码。

SF=0，TCP回话正常完成；

S1=1，连接建立，却没有终止；

S2=2，连接建立并被发起方关闭，接收方没有响应；

S3=3，连接建立并被接收方关闭，发起方没有响应；

S0=4，一方发出SYN，另一方没有应答

SH=5，发起方发出一个SYN和FIN，却没有收到SYN和ACK应答；

OTH=6，没有SYN的大流量通讯；

RSTO=7，连接已建立，发起方发送RST，放弃连接；

RSTR=8，连接已建立，接收方放弃连接；

TST0S0=9，发起方发出一个SYN和RST，却没有收到SYN和ACK应答；

RSTRH=10，接收方发送一个SYN和RST，却没有收到从发起方发送的SYN；

REJ=100，连接企图被拒绝

1. Src\_bytes：从发起方到接收方的数据比特数。
2. Dst\_bytes：从接收方到发起方的数据比特数。
3. land：发起方的地址和接收方地址是否一样。
4. Wrong\_frament：错误分片个数
5. Urgent：带外数据包个数。

3.1.2.2 内容特征（content features）

考虑到R2L和U2R攻击一般潜伏在数据包的有效负荷部分，又因为从单一的数据包分析和正常连接没有什么区别。内容特征反应了在数据包负载部分可能的入侵信息，如num\_failed\_logins说明失败登录次数信息，这对于检测guess\_passwd之类的R2L攻击十分有效，但是另一方面，13维的内容特征并不能反映数据包负载部分的全部特性，因此，这样的特征选择方法，对特洛伊木马类型的攻击，依然无法检测。

1. Hot：访问系统敏感目录和文件的次数
2. Num\_failed\_logins：登录失败次数
3. Logged\_in：是否成功登录，成功为1，失败为2
4. Num\_compromised：出现compromised情况的次数。比如出现“file/path not found”错误的次数。
5. Root\_shell：是否获得了根shell，成功为1，失败为0。
6. Su\_attempted：是否出现“su root”命令，是为1，否则为0。
7. Num\_root：根用户访问次数。
8. Num\_file\_creations：创建文件操作次数
9. Num\_shells:shell使用的次数
10. Num\_access\_files：访问文件操作次数
11. Num\_outbound\_cmds：在FTP绘画中的Outbound命令出现次数
12. Is\_host\_login：登录是否属于授权主机列表，YES=1，NO=0。
13. Is\_guest\_login：是否为“guest”登录，YES=1，NO=0。

3.1.2.3 两秒钟内的流量特征（traffic features computed using a two-second time window）

研究表明，网络攻击事件通常在时间上具有很强的相关性，特别是对于DOS和Probing等攻击来说，在很短的时间内对同一主机会有多个连接。因此，考虑在检测数据中加入基于时间的统计特性，将会更好的反映攻击数据包之间的内在联系。采用时间窗的概念，即针对每一条连接记录，统计出在之前指定的时间内的连接记录与当前连接记录在属性上存在的某种联系。时间窗宽度定为2秒。

1. [] http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201801/P020180131509544165973.pdf [↑](#endnote-ref-0)
2. [] http://www.cert.org.cn/publish/main/46/2012/20120330183838603351566/20120330183838603351566\_.html [↑](#endnote-ref-1)
3. [] 俞研.基于数据挖掘的网络入侵检测技术研究. 博士学位论文. 南京大学计算机科学与技术系.2006 [↑](#endnote-ref-2)
4. [] [↑](#endnote-ref-3)
5. [] ISO 1798-2 Information processing systems-Open Systems Interconnection Reference Model-Part 2:Security Architecture,International Organization for Standardization,1989 [↑](#endnote-ref-4)
6. [] [↑](#endnote-ref-5)
7. [] [↑](#endnote-ref-6)
8. [] [↑](#endnote-ref-7)
9. [] 项国富. 虚拟计算环境的安全监控技术研究[D].华中科技大学,2012. [↑](#endnote-ref-8)
10. [] Kumar S. Classification and Detection of Computer Intrusions [D]. Lafayette: Purdue University, 1995 [↑](#endnote-ref-9)
11. [] 卿斯汉 ,蒋建春 ,马恒太 ,文伟平 ,刘雪飞.入侵检测技术研究综述[J].通信学报,2004(07):19-29. [↑](#endnote-ref-10)
12. [] Anderson J P. Computer security thread monitoring and surveillance[R]. Fort Washington, PA. 1980 [↑](#endnote-ref-11)
13. [] D.E. Denning, An Intrusion Detection Model, In IEEE Transactions on Software Engineering, 1987, 13(2):222-232 [↑](#endnote-ref-12)
14. [] S.E Smaha, Haystack:An Intrusion Detection System, Proceeding of the IEEE Fourth Aerospace Computer Security Application Conference, Orlando, FL., DEC. 1998 [↑](#endnote-ref-13)
15. [] M.Sebring,et al,Expert System in Intrusion Detection: A Case Study, Proceedings of the 11th National Computer Security Conference, Baltimore, MD,Oct,1998 [↑](#endnote-ref-14)
16. [] H.S Vaccaro, GE.Liepins, Detection of anomalous computer session activity, Proceeding of 1989 Symposium on Research in Security and Privacy, Oakland, CA., May 1989 [↑](#endnote-ref-15)
17. [] J.R. Winkler, WJ. Page, Intrusion and Anomaly Detection In Trusted Systems, Proceeding of the Fifth Annual Computer Security Applications Conference, Tucson, AZ,Dec,1989 [↑](#endnote-ref-16)
18. [] Heberlein L T. A network security monitor[A]. Proceeding of the IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA:IEEE, 1990, 296-303 [↑](#endnote-ref-17)
19. [] Jackson K, Dubois D, Stallings C, An Expert System Application for Network Intrusion Detection[A], Proceeding of the 14th Department of Energy Computer Security Group Conference[C], Concord, CA. Unite States Department of Energy(DOE), 1991 [↑](#endnote-ref-18)
20. [] Snap SR, Brentano J, Dias G V, A System for Distributed Intrusion Detection[A], Proceedings OF the IEEE COMPCON91[C], San Francisco, CA:IEEE,1991,Page 170~176 [↑](#endnote-ref-19)
21. [] J.S Balasubramainyan, J.O. Garcia-Femandez,D.Isacoft. et al, An Architecture for Intrusion Detection Using Autonomous Agents, Department of Computer Sciences, Purdue University, Coast TR 98-05, 1998 [↑](#endnote-ref-20)
22. [] R. Andersion, A.khattak, The Use of Information Retrieval Techniques for Intrusion Detection, Proceeding of RAID’98, Louvain-la-Neuve,Belgium, Sept.1998 [↑](#endnote-ref-21)
23. [] Lee W, Stolfo S. Data mining approaches for intrusion detection.7th USENIX Security Symposium, San Antonio, TX,1998 [↑](#endnote-ref-22)
24. [] Warender C, Forrest S, Pearlmutter B. Detecting intrusions using system calls:alternative data models[A]. Proceedings of the 1999 IEEE Symposium on Security and Privacy[C]. Berkely,California, USA:IEEE Computer Society, 1999:133-145 [↑](#endnote-ref-23)
25. [] 戴英霞,连一峰,王航. 系统安全与入侵检测[M]. 北京:清华大学出版社，2002 [↑](#endnote-ref-24)
26. [] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html [↑](#endnote-ref-25)
27. [] 张新有,曾华燊,贾磊.入侵检测数据集KDD CUP99研究[J].计算机工程与设计,2010,31(22):4809-4812+4816. [↑](#endnote-ref-26)