

基于虚拟专用网络技术在计算机网络信息安全的分析

周康乐

(南昌理工学院 江西 南昌 330511)

[摘要]随着信息网络的全面普及,信息安全成为社会重点关注问题,网络攻击与信息泄露等成为安全隐患,对人们的隐私信息造成巨大威胁。基于此,本文围绕虚拟专用网络技术(VPN)展开研究,首先简单阐述了虚拟专用网络技术与计算机网络信息安全风险,并在此基础上完成应用分析,旨在充分发挥虚拟专用网络技术保护价值,营造安全稳定的网络环境。

[关键词]虚拟专用网络技术; 计算机网络; 信息安全

[DOI] 10.12252/j.issn.2096-627X.2020.07.388

引言

根据国家互联网应急中心(CNCERT/CC)《2019年中国互联网络网络安全报告》中显示,2019年全年捕获计算机恶意程序超6200万个,日均传播次数高达824万余次,受到攻击的IP地址约6762万个,此外据CNCERT/CC抽样监测数据显示,我国4万余台IPv6地址计算机受到安全侵害,同时2019年数据泄露问题愈加频繁,涉及社会各个行业,由此不难看出网络信息安全已迫在眉睫。

一、虚拟专用网络技术

虚拟专用网络技术又称VPN,是现阶段加强网络信息安全的重要手段,其主要分为加密和认证、隧道技术、密钥安全关联等技术。

(一) 加密和认证

从虚拟专用网络技术角度来看,加密主要围绕数据进行加密计算,通过加强数据保护规避窃听、泄露等问题,数据加密同时可阻挡部分网络入侵,认证主要是指身份认证与用户认证,借助IP地址通讯获取信息接收者真实信息,结合AH协议等手段保障数据来源与信息完整。在现阶段虚拟专用网络技术发展,加密与认证逐渐成为基础性安全防护技术,通常结合使用,在ESP协议基础上保障数据可靠。

通过AH协议完成认证,主要功能为保障数据传输安全,其单独使用时并不具有防窃听效果,其于信息数据包内增设身份认证信息,并将身份认证标准化数据处理,将其设置在IP地址内,以此实现完整保护,由于其单独使用并不具备防窃听功能,因此其对于非隐私信息的传输更为适用。ESP协议以功能为依据划分为头部与尾部,其中头部主要用于加密与索引,有信息发送者与接收者协商完成决定加密策略,而尾部主要用于信息验证,并通过其序列号完成验证对比,以此实现数据安全保障,其中加密算法主要由64位输出数据组成,其加密强度较高。

(二) 隧道技术

隧道技术是虚拟专用网络技术的核心内容,将传输数据封装保密,从协议A传输至指定协议B,现阶段隧道技术广泛使用第三层隧道,其中GER与IPSec在网络信息中最为常用。GER主要来源于地址与目的地址实现隧道定义,在IP帮助下用户可完成信息封装,此外可借助公用IP网络使用保留地址,并于网络内隐藏自身IP地址;IPSec隧道主要为保障信息通讯安全完成的协议包,能够实现IPv6的数据迁移,其具备开放性、广泛性特点,相对于GER而言,其在虚拟专用网络技术中安全功能更为全面,可实现网络层数据保护,围绕机密信息构建网络安全机制,图1为虚拟专用网络技术中IPSec信息处理流程图。从隧道技术角度来看,IPSec可在隧道模式、传输模式下运行,隧道模式下的将数据封装,并传输至安全IP内,而传输模式则是为保障网络地址间的传输安全,此两种模式成本较高,但相对应的其安全指数较高,同时其各节点间的缺乏可控性,因此可在虚拟专用网络技术认证与加密机制作用下完成数据传输^[1]。

(三) 密钥安全关联

在虚拟专用网络技术中,密钥技术中对称加密(私有加密)与非对称加密(公共密钥)应用最为广泛,对称加密由信息传输方与接受方设定私有密钥,以此实现信息加密,对称加密系统运行时,默认信息传输双方已完成密钥交换;非对称加密主要由系统自动为信息传输双方生成密钥,由存放于公共区的公钥和私下保存的私钥组成,在信息传输时两种密钥各有功能,例如:A传递信息至B,A需于公共区内获取公钥后,对信息进行加密处理后发送,B收到加密信息后,可运用私钥完成解密,以此实现信息保护,规避传输过程的泄密问题。

二、计算机网络信息安全风险

现阶段计算机网络信息安全受到多方威胁,例如:网络攻击、恶意入侵、病毒植入等,可造成信息篡改、数据窃取、节点冒充等安全风险。

信息篡改主要分为内容篡改、时间篡改、顺序篡改,内容篡改主要为运用网络技术手段对传输信息删除与内容修改,甚至可能存在内容插入问题,能够直接影响信息精确度,而时间篡改主要分为信息延迟传输或重放,在某些特定环境下,时间篡改可造成巨大损失,顺序篡改主要为重组消息序列码,打乱其排序导致其数据失真;数据窃取主要针对信息传输目的地址完成数据窃取,例如窃取信息系统登录口令与用户信息,以此获取系统控制权,继而窃取机密数据;节点冒充主要指截取网络中间节点控制权,或运用网络技术手段自建节点冒充入网系统进行篡改,节点冒充形式不仅可非法获取网络信息还可在节点控制下发送错误信息,此外可对目的地址发送病毒,造成其网络瘫痪现象。

三、计算机网络信息安全中的虚拟专用网络技术应用分析

为了更好的保障计算机网络信息安全,以下基于虚拟专用网络技术展开分析,从IP地址统一编码、多层级数据交换、信息数据加密算法、信息安全传输封装、网络防火墙部署五个方面进一步探讨。

(一) IP地址统一编码

IP地址统一规划是基于虚拟专用网络技术进行网络信息安全保护的基础,需秉持系统化、标准化、科学化的原则完成信息分类,并才网络编码技术支持下保障信息传输质量与安全。以高校图书馆信息建设为例:其IP地址范围仅限于局域网,在展开各级图书馆阅览室分中心网络连接时,可将其私有地址统一化设计,如10.0.0.0,由于高校图书馆涉及各院系藏书资源,是校内师生学习与科研质量的保障,因此需在虚拟专用网络技术基础上完成IP地址统一编码,以此保障信息安全,除图书馆私有地址统一化外,需组建相应的网络组织结构,应结合高校图书馆访问权限形成组织结构从属关系,并结合VLSM、CIDR等技术完成科学资源分配与保护,以信息资源分类组成IP地址空间^[2]。IP地址的统一分配缩短信息传输过程,实现快速传递可规避部分信心拦截等安全问题,同时当信息数据遭受网络入侵与攻击时,一旦IP地址发生变化,则可及时发现并拦截,可有效提高网络信息安全质量。

(二) 多层级数据交换

基于虚拟专用网络技术完成网络信息安全保护时,可借助多重数据结构完成信息保护,同时在现阶段网络问题中,常因自然物理因素(如火灾、地震等)导致网络存储信息丢失,因此可借助网络系统连接完成信息同步,并设置映射关系实现信息对应组合,这就要求运用虚拟专用网络技术实现安全保护时,需基于交换与传递标准进行映射数据对照,不仅可保障信息精确度,运用映射数据对比可保障原始数据安全,同时可按照数据类型完成分析,并结合其传输位置加强管理权限控制,充分发挥虚拟专用网络技术价值,保障网络信息安全。

(三) 信息数据加密算法

信息数据加密算法是保障网络安全的基础,可借助虚拟专用网络技术加密算法完成明文数据转换,并通过特定密钥解密后方可完成信息读取,明文作为数据原始形态,在虚拟网络系统中其易受到攻击或窃取,当明文经过虚拟专用网络技术加密处理后将成为密文,以此实现数据保护,在解读信息过程中,需再借助虚拟专用网络技术完成解密,因此这就要求信息传递双方均掌握虚拟专用网络技术。除此之外数据加密过程可根据信息内容机密程度设置不同密级,在技术支持下完成抗拦截、抗篡改功能,同时规避非法访问、信息复制等信息泄密问题。

实现加密算法是一般运用单钥密码、签名密钥、哈希算法、量子密码技术。单钥密码主要运用单一密钥完成信息加密,主要以对称密钥为表现形式,相较于其他加密算法而言,其速率较快,在大量数据保护是运用最广,此过程主要采用单一密钥,因此加密完成后信息传输双方即可获取相同加密、解密信息,因此单钥方式加密安全完问题主要在于密钥保护,而非加密信息保护,因此需借助IV协议等技术流程完成密钥保护;签名密钥主要由运用在非对称密钥加密中,有上述介绍中可知,需公钥与私钥共同作用下完成信息解密,而签名密钥主要针对私钥展开,通过签名密钥进一步保障网络信息安全,同时签名密钥仅需接受公钥验证后方可使用,这就保障了非对称密钥的专属性,不可被其他无关用户窃取,公钥与签名私钥验证过程中,其通信对话具有唯一性,彰显网络信息安全,现阶段签名私钥加密算法一般采用DSA、RSA展开;哈希算法主要通过二进制完成固定长度的加密,其中较小的二进制加密则被称为哈希值,其具备数据唯一、数值紧凑特点,主要针对明文信息进行哈希数值更改,将其分散排列成为不同表现形式,例如A向B传递信息,双方均具有哈希原始数据,B接收信息时可将信息与哈希数值对比,将信息内容分散解读,以此读取其真实内容,在现阶段MD5、HASL在哈希算法中最为常用;量子技术加密可分为单光子光纤一级加密与量子计算机加密,量子计算机加密主要运用超大规模计算系统完成密钥分解,随着技术的发展逐渐形成了单光子光纤一级加密,其速度进一步提高,但受到技术研发限制,其对网络攻击行为进行检测时,易出现不准确现象,因此并未大规模采用,但其为未来虚拟专用网络技术保障网络安全的主要发展方向^[3]。

(四) 信息安全传输封装

信息封装是防止密钥泄密问题的进一步保障,一般借助打包封装形式完成信息保护。打包封装的主要功能在于拦截网络信息访问行为,在此过程中可实现高质量互联网数据保护,并借助虚拟专用网络技术实现报文交互与分析,将打包封装系统接收到明文信息后,需按照所设定的加密要求完成报文数据提取与记录,按照相应规格设置打包指令,打包信息与密钥同时保存,便于后续报文解密与读取,此外为保障信息完整性,需按照特定算法标准完成核算,最后将打包信息与密钥同时封装,最大化保障信息安全。

打包处理主要包括系统服务器与打包工具,两者相辅相成,系统服务器主要为保证正常信息存储与传输,并维护网络安全环境,信息于数据库内存储时,需完成信息处理,将其加密算法与节点一一对应,当完成用户身份认证后,通过打包工具完成报文分析,此时系统服务器将会展开二次验证,进一步提高网络安全保障^[4]。

(五) 网络防火墙部署

网络防火墙部署是展开全面虚拟专用网络技术应用的基础,通过封包过滤完成协议设置,只有符合特定标准规范的信息方可穿过防火墙,而相关标准可由管理人员结合信息存储内容与传递用户展开修改,现如今一般从源地址、源端口号、目的IP端口号、目的IP地址等信息判断是否用于访问资格,除此之外的TTL值、来源域名等通讯协议均可通过过滤后穿越防火墙。

从虚拟专用网络技术角度来看,可从采用以下方式进行除此防火墙部署:第一,围绕内网终端展开设置,防火墙位置置于内网终端前,此方式安全性能较高,虚

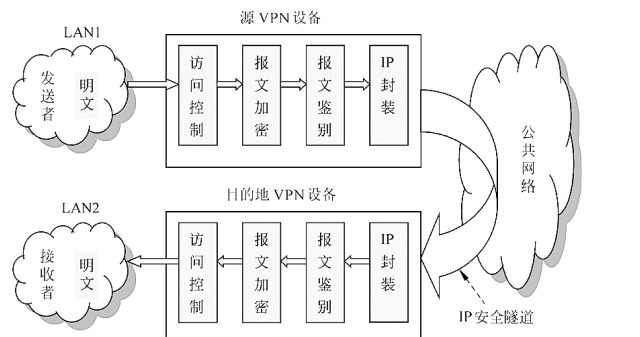


图1 IPSec信息处理流程图

拟专用网络设备及防火墙完成串联,此方式虽安全性较高,但其易受到网络非法攻击;第二,在内、外网终端内完成防火墙部署,其中防火墙具有隔离保护作用,虚拟专用网络设备易受到防火墙保护,但在防火墙部署时单独配置流量通道,以此保障虚拟专用网络技术能够发挥作用。经过各项实践对比,第二种方式在网络安全保护中效能更高。

结束语

综上所述,现阶段网络安全问题种类日益增加,其频率呈上升趋势,为更好地维护网络信息安全,可运用加密认证、隧道技术、密钥安全关联等虚拟专用网络技术缓解此类问题,通过IP地址统一编址加强安全防护,多层次交换规避部分网络攻击,同时在加密算法、传输封装、防火墙部署应用下,实现多元化网络信息

安全防护,切实保障虚拟专用网络技术发挥应有作用。

参考文献

- [1] 张志花. 基于网络信息安全技术管理的计算机应用探究[J]. 网络安全技术与应用, 2020(09): 8-9.
- [2] 李君. 数据加密技术在计算机网络信息安全中的应用[J]. 南方农机, 2020, 51(15): 196-197.
- [3] 王颖. 基于信息挖掘技术的网络信息安全风险预测[J]. 兰州文理学院学报(自然科学版), 2020, 34(04): 57-61.
- [4] 雒贵芳. 大数据时代计算机网络信息安全防护分析[J]. 网络安全技术与应用, 2020(05): 76-77.

小学语文群文阅读中读写结合之策略

宋方艺

(新疆精河县第一小学 新疆 精河 833300)

[摘要]随着近些年我国教育理念的不断转变,对于教育改革工作不断深入推进,小学教学要求的变化也极为明显,尤其是对于小学语文教学工作的要求,语文是小学教学中极为重要的一项科目,对于如何提升小学语文的教学时效性也受到了社会各界以及教育工作者的重视。小学语文群文阅读中实施读写结合教学策略,是为广大的小学语文教师提供了一条全新的教学发展道路,对于学生阅读能力、以及写作能力的提升极为明显。

[关键词]群文阅读;小学语文;读写结合

[DOI] 10.12252/j.issn.2096-627X.2020.07.389

在实际的教学发展过程中,小学是学生学习和成长的最重要的阶段,这一阶段,也是学生学习观念和学习系统形成的基本阶段。在这一阶段所开设的课程中,语文是最为基础的,因为语文的学习可以帮助学生了解和拓展学科知识面,同时也为学生学习其他学科打下基础。在实际的语文教学过程中,阅读教学是语文教学的重要组成部分。因此,为了给学生提供更好的阅读教学内容,鼓励他们更好地开展阅读训练,基于阅读和写作教学方法相结合的群文阅读教育活动脱颖而出,给相关教学人员带来了许多新的教学思路、以及教学方向。与此同时,在实际的教学评估中,无论是高考还是中考都非常重视阅读,新教材中的阅读量也大大增加,为了让孩子们在有限的时间里增加阅读数量,学习更多的知识,群文阅读教学吸引了大家的重视^[1]。针对小学语文群文阅读教学中实施读写结合的意义和以及实际的实施策略进行探讨。详细探讨内容见下文:

一、小学语文群文阅读教学中实施读写结合的意义

在小学语文群文阅读教学过程中,对学生实施读写结合,可以对学生的阅读量进行有效增加,对于学生的综合语文素质、以及综合能力也有极大的提升,在实际的群文阅读教学过程中,采取读写结合措施,可以让学生在参与到群文阅读活动的同时,对其阅读理解能力进行加强,并增强学生通过写作表达思想的能力。

在小学语文群文阅读教学的过程中,教师选择实施读写结合方案,对于学生的教学效果、以及所得教学质量均可大幅度提升,这是由于教师在实施读写结合的过程中,会对自己的教学计划和目标更为清楚,同时在进行群文阅读教学时,所需要的文本阅读量也会增加,而在这种情况下,教学所涉及的范围也会逐渐增加,教师就更需要加强自己的阅读范围,并对自身的阅读能力和教学能力进行提高。

二、小学语文群文阅读教学中实施读写结合的策略分析

1、加强重视程度

在实际进行教学的过程之中,教师需要加强对读写结合教学的重视,这有助于教师更好地实践群文阅读教学。在设计和安排教学内容过程中,教师注重阅读和写作教学方法的结合,可以帮助教师更好的了解和掌握教学内容,更好的设计和安排教学环节,从而使教学内容更符合实际的学习水平的学生,这样可以更有效地进行教学,并完成教学任务和教学目标,学生学习水平也不断提高^[2]。

2、对教学方式方式进行创新

教学方法的多样化,也是促进读写教学在小学语文群文阅读教学活动中的一种有效途径。在实际的教学发展过程中,教学方法的多样化可以帮助教师展示教学内容,并帮助教师更好地组织和开展教学,吸引学生积极参与教学活动,更快地促进学生理解和掌握课堂的内容,实现持续发展,提高他们的学习水平^[3]。以部编版教材六年级中《慈母情深》《父爱之舟》这两篇课文,课文分别描述了父爱和母爱,课文对于母爱、以及父爱的描写十分感人,为了进行这一单元课文的教学,可以借助多媒体设备,播放图片、视频以及音频,对相关的父爱、母爱故事进行辅助说明和教学,帮助学生从课文中所描述的情景进行直观感受,学生在感受课文中所描述的情况后,可以在教师的指导下,对自己所感受到的父爱、母爱进行回忆和表达,加强课文学习效果的同时对学生的口语能力进行锻炼。

3、提高教师专业水平

提高教师的教学水平也是将读写更好地融入小学语文读写教学活动的一种方法和策略。这是因为在实际教学过程中,教师的持续改进和发展的教学水平可以帮助他们更好的掌握和理解教学内容,更好地理解并完成教学任务、以及教学目标,更好的掌握学生的学习水平和学习状态,从而引导学生安排教学内容更加科学和合理,实现教学效率和教学质量的不断提高。在群文阅读的实际教学过程中,为了更好的运用这种阅读和写作模式,教师也可以通过交流经验,向其他优秀的教学工作者学习,更好的进行沟通和交流。这使得教师教学经验更加丰富,教学内容更加可行,提高了教师的教学水平,对学生产生了更好的教学效果。

4、仿写练习

群文体阅读不是大众阅读,也不是单一主题的阅读。它是近年来悄然兴起的一种突破性的新的阅读教学模式。它是由教师和学生结合一组文章,以特定的方式围绕主题引导学生阅读和阅读,并分析其中异同,加强学生阅读的深度和广度,锻炼和提高学生的阅读能力和思维能力。因此,为了实现“读写结合”的教学目标,教师在阅读教学过程中,需要确保教学内容与课程标准相一致。通过模仿提高学生的写作能力。

对同一主题的多篇课文进行探索性教学,写作来自生活。教师要想在写作过程中保证学生有足够的写作材料,就需要让学生从生活中积累语文写作材料,观察身边环境以及发生的故事,让学生在日常生活过程中紧密围绕一个话题进行创作。在群文阅读教学过程中,教师选择能够指向对多元文本丰富的人文思想内涵的理解、感知和反思的文章,引导学生对多元文本的结构、概念、语言、风格等语言形式进行欣赏、评价,并进行学习和应用,使群文阅读教学具有明确的语文学科目标和有效价值,更有利于学生阅读能力的整体培养和发展,使学生在阅读学习的过程中提高自己的写作能力。

结语

综上所述,小学语文教育的发展,会对学生的后续学习和实际生活产生影响,小学新时期中语文教师,在进行教育的过程中应注意教学方法的改进和创新,并借助群文阅读和写作教学相结合,来实现对学生的阅读能力和写作能力进行培养的目的,同时鼓励、引导学生提高阅读和写作的兴趣,为学生未来的发展奠定了基础。

参考文献

- [1] 邵素梅. 小学群文阅读读写结合实践研究[J]. 大观, 2016, (3): 247-247.
 - [2] 杨滢. 浅谈小学阶段读写结合的群文阅读教学策略[J]. 语文课内外, 2020, (3): 176.
 - [3] 张芬芬. 以“课内外阅读”构建小学群文读写结合课堂教学新模式[J]. 课程教学研究, 2017, (2): 229-230. DOI: 10.3969/j.issn.2095-3089.2017.02.227.
- 作者简介:
宋方艺, 1977, 2女 汉族 山东省菏泽市 大专 一级教师 研究方向: 小学语文 群文阅读。

基于教材的范文仿写法在七年级英语写作教学中的应用

陈舒静

(驻马店市第三中学 河南 驻马店 463000)

[摘要]英语写作可谓是大多数初中学生在英语考试中薄弱的环节,许多学生在开始学习英语时,就十分畏惧写作。当中学时期,许多学生在英语写作方面付出了大量的时间和精力,但却很难有所提高,与此同时,教师的英语写作教学也存在教学形式单一等缺陷。那么,我们应该怎样提高写作教学设计的有效性使学生的英语写作水平在初一阶段得到一定程度的提高呢?本文主要对七年级英语仿写写作课堂有效性的提升方法进行探讨,希望能对七年级英语仿写写作学习带来帮助。

[关键词]范文仿写;七年级英语;英语写作教学

[DOI] 10.12252/j.issn.2096-627X.2020.07.390

引言

随着我国经济水平正在不断提升,教育也随之创新和发展,英语是初一的重要组成部分,受传统应试教育的影响,有许多教师依然用传统的讲授方法进行教学,忽视学生数学能力生活化的培养,这样就会导致学生的实践能力与理论知识不能相结合所以就不能更好的去掌握数学知识,不利于学生的未来发展,因此,在初中英语课程中,教师要根据学情,去引导学生自主学习数学知识,并且灵活运用在生活中。

一、仿写在七年级英语的意义

英语老师都在一线工作,有着多年的教学经验,在教学方面都有着靠自己平时花了大工夫讲解、吃透课文,到写作时却舍近求远,忽视了我们身边最直接的、可利用的素材,这是非常错误的。我们英语教材上的阅读材料名篇、佳作,我们要让学生掌握这些短文的写作技巧,做好知识的迁移,学以致用,形成自己的写作成果。英语作文是最令我们教师和学生头疼的事,学生不会写,作能力就成了困扰老师和学生的问题。有一次我班一位同学月考中一篇仿写作文引起了评卷老师的兴趣,给出了20分的高分(总分20分),我从中受到启发,所以,在平时的写作训练中,我便要求学生先从仿写课文入手,逐步培养学生快乐写作的信心。英语写作必