基于大数据时代的计算机网络安全防范措施分析

刘继强

（泰安市泰山网络传媒有限公司，山东　泰安　271000）

摘　要：在当今时代背景下，人们已经进入大数据时代，计算机在各个行业中得到广泛应用，不仅改变了人们的生活方式，其工作方式也发生了很大变化。与此同时，互联网传播速度越来越快，人们信息储存也有所增多，在享受大数据带来便利的同时，人们的计算机网络安全防范意识也在逐渐加强，以尽可能地减少计算机网络带来的风险。基于此，本文从理论入手，简要分析了在大数据时代下计算机网络安全存在的问题，提出了计算机网络安全的防范措施，以为网络安全建设提供理论基础。

关键词：大数据时代；计算机；网络；安全防范

中图分类号：TN915.08　　**文献标识码：**A

0　引言

在今天，计算机技术得到了广泛的应用，与此同时，人们对大数据有所认知，在此背景下计算机不仅改变了人们的生活、工作、学习的方式，而且带给了人们便利，信息保存与传输速度有所提高，存储空间得到扩大，同时也减少了人为记忆的相关内容[1]。但是在计算机网络的有效应用中却存在着诸多安全隐患，所以要基于现状做好对大数据时代计算机网络安全防范的研究。

1　大数据的基本概述

1.1　时代特点

毋庸置疑，大数据自出现以来带给了人们全新的发展态势，人们也迈入了信息化时代。现如今，在人们生活中，衣食住行均与计算机有着密切的关联性，与此同时，社会在不断发展，相应的数据也有所增多，为将数据的价值充分发挥出来，要做好数据的收集、分析与存储，如果选择传统的存储方式会存在缺陷，但是在大数据时代可以通过计算机进行数据的融合与整理，保证数据的本身价值，增强数据信息的整体利用率。

在大数据时代的有效应用下，人们的生活节奏越来越快，压力越来越大，诸多网络不法分子出现，严重威胁了网络的安全，甚至还引发了社会问题。所以大数据带给人们的价值具有双面性，人们要正确地判断，及时地辨识，做好正确引导，将大数据的正当价值发挥出来[2]。

1.2　意义和特点

大数据实现了信息的转化，具有快捷性与全面性，在大数据时代人们借助于计算机技术，无论其生活还是工作均带来了便利，这对推动经济的发展也有所帮助。通过大数据可以实现海量信息的整合，或利用数据库技术做好信息的分类，有效地提升数据资源的整体利用率[3]。从特点上分析，大数据具有开放性，不会受到时空所带来的限制，可以随时随地获取信息资源，但是在整个业务过程当中会受到客观因素与主观因素带来的影响，引发各类安全隐患。同时大数据具有唯一性，而这也是广泛应用的原因之一。

1.3　大数据与网络防护的关系

在信息时代数据的传递越来越快，存储也逐渐地呈现出多元化，大数据的有效应用为人们改变了信息检索与查询所存在的缺陷与不足，能够实现对数据的分类、提取、统计，满足了精细化的发展要求。然而每天每时每刻会产生海量的数据，计算机的实效性与功能性也得到了完善，在大数据进行数据整理、分类、归纳、统计时，促使各类程序在互相配合当中实现数据的全面统一[4]。然而整个过程极易发生漏洞，如果某一个程序出现漏洞还会产生毁灭性的打击，甚至还会引发安全事故。在大数据时代需要发展思维，紧跟时代发展的步伐，做到与时俱进，对于机密或隐私的信息更要做到严防死守，以此在增强资金安全性的同时也能为构建和谐社会奠定基础。

2　计算机网络安全问题的表现

2.1　计算机系统本身问题

一般而言，计算机系统本身所存在的问题主要是指硬件与软件，且在大数据时代，如果软硬件未及时

更新，则无法满足时代发展的要求，尤其在运行中还会出现漏洞，导致信息安全隐患的出现。除此之外，在运行过程中，计算机网络是人为设定的框架模式，需将其作为主要的载体进行数据的传输，但是单纯地从设计角度分析，在进行软件或硬件开发设计时，因为软件自身存在容错性问题，所以会导致系统运行出现问题，容错性问题是值得关注的问题之一，这是系统拓展的载体，同时也与网络架构所存在的服务问题有所关联。

从另外一个角度分析，因计算机系统自身存在问题，所以在安装软硬件时无法做到软件驱动，数据信息传输会呈现出错误指令行为，会导致数据传输风险加大。假如用户在利用计算机过程中下载了诸多的软件，其安全性无法保证，在数据传输当中会出现诸多风险，这不仅会对计算机的本体产生破坏，甚至还会出现数据丢失等一系列问题。

2.2 受到病毒或黑客所带来的影响

自计算机诞生以来，病毒与黑客始终存在，计算机时代下数据信息传输越来越快，且高效率的数据传输逐渐推动了产业结构的有序发展，甚至在近几年衍生出了基于数字化与信息化的经济链，同时计算机系统经过对各类软件的应用，存储空间会越来越小，但是可以实现对用户自身的身份界定，能够对数据对接，在该基准下可以达到完善的网络体系，对用户的诸多网络行为加以约束。然而正因为如此，会为诸多不法分子提供了可乘之机，比如可以通过贩卖用户的信息获取经济回报，或者在受到病毒侵袭或黑客攻击下，导致系统出现瘫痪，还有诸多不法分子在进行定位时会选择通过邮件轰炸或监听数据的方式影响用户的生活，对网络程序进行非法篡改，形成网络资源流失，引发经济风险[5]。

病毒是影响计算机使用安全性的主要载体，如果存在病毒则会对数据信息造成威胁，甚至病毒在侵入计算机设备之后还会对网络产生危害，不仅会影响计算机设备的工作，甚至会引发经济损失。

2.3 用户防范意识存在问题

计算机网络系统在运行中始终处于相对静止的状态，在得到用户指令后形成自动化操作。用户是计算机使用的主要制定者，且在计算机中的各类操作行为会引发安全问题，用户在使用计算机设备时如果缺乏安全意识，在发生系统故障时大多数用户会选择直接关机的方式，并未选择专业的软件进行全力检测。同时，大数据时代计算机中的数据呈现出海量性，用户缺乏判断能力，无法对具有安全隐患的信息进行甄别，如浏览网页时导致带有病毒的信息弹出，并经过防火墙进入到计算机系统内部，出现病毒感染。

2.4 缺乏完善的网络监管制度

制度决定计算机应用的可行性，在大数据时代计算机的使用带给了人们便捷，无论是信息的获取还是分享，演变得更加快速，且数据呈现出海量性，与此同时，会出现诸多危害人类利益的信息。尤其在近几年社会与科技的发展下，关于网络方面的监管制度并不完善，这为安全问题带来了隐患，正因为网络监管制度不完善，所以诸多人员会通过网络传送不良信息，甚至还会对国家的机密进行盗取[6]。

2.5 网络协议存在缺陷

网络需连接不同的计算机与服务器，且对象不同，连接时所需要的传输控制协议也有所不同，而这便是我们常见的IP网络协议。就目前而言，在受到多方面因素所带来的影响下，网际协议缺乏完善性，不仅未制定保护机制，并且在计算机数据传输方面也存在不确定性，这对用户的数据安全产生了威胁[7]。当前传输控制协议是主要的形式，处于完全公开的状态，其他用户能够通过远程的方式访问他人的电脑并获取相关的信息，甚至还可以为黑客的侵入带留下“后门”，如此发展趋势则会严重影响网络的安全。

3 基于大数据时代做好计算机网络安全防护的措施

大数据已经成为了计算机网络的主要发展模式，在新时期不仅要认清大数据的重要意义，也要做好计算机网络安全体系的构建，其中网络安全防护措施可以从以下几点入手。

3.1 做好网络身份安全验证工作

通常，计算机初期阶段大多数用户并不具备安全防范意识，尤其在双方不需要互相认证的环节下安全性成为值得考虑的问题之一。在未来的发展中可以将网络身份安全验证技术融入其中，这样不仅可以进一步保证用户的安全性，也能为广大用户在上网时带来安全保障。就目前而言，关于身份安全验证的技术趋于成熟化，并得到了有效的应用，据了解仍旧有诸多不良网站的存在与发展，无法实现用户身份的全面验证，对此，要从政府层面入手，对网络信息进行备案，尤其在用户与服务器构建连接的时候采取双重分身验证的方式，如此才能够进一步增强其安全性与全面性。

3.2 制定网络入侵检测体系

时代的不断发展下，网络发展的速度越来越快，其隐患也越来越多，因人们的生活已离不开网络，所以在新时期，要加强对大数据的应用，制定完善的网络入侵

检测体系，尽可能地减少信息的泄露以及被利用。其中该检测体系要从两个方面入手，一方面是制定早期预警机制与精准辨别机制，这样可以为人们提供一定的参考依据，比如DDOS攻击事件，可以应用大数据实现对域名系统协议访问日志以及原始数据、路由器分配服务器的归纳、整合，对主机攻击源加以检测；另一方面也要做好分布式拒绝服务攻击路径的检测，可以选择模拟攻击的方式获得相应的数据，进而完善检测体系与系统，为网络的安全性保驾护航。

3.3 完善安全性信息加密技术

在登录计算机时离不开账号且需输入密码才可成功进入，这便属于加密技术，当然诸多加密技术过于简单，黑客通过入侵可以解密，窃取信息，为保证用户的财产安全，要采取更为高效的安全信息加密技术，实现多层加密，做好对信息传输的安全防护。①可以选择节点加密，主要是在信息的节点处应用密码装置，并与节点机相互连接，如此在数据读取当中可以通过加密提高安全性，减少数据盗取现象的发生。②可以选择网络连接加密技术，主要是通过与服务器构建连接之后，进行数据节点的传输，在每一个节点均设计加密程序，每一个节点均需进行解密，采取多层保护增强安全。③可以选择数据首尾加密，在运行前与运行后进行加密，特别是数据传输时通过加密的方式提高安全性。

3.4 增强防火墙的性能

防火墙是计算机中的主要内容，大多数计算机自带防火墙，无论是数据的输入还是输出均需经过防火墙进行筛选，当筛选信息不符合安全级时会被阻拦，如此可以减少不良信息的入侵[8]。同时在应用过程中，用户要根据实际的情况做好防火墙安全等级的调整、参数的设置，如果属于机密信息，那么则要提升防火墙的级别，无论是内网还是外网，在进行连接时都要进行监测，将互联网上的各类活动加以记录，如出现可疑问题能够在最短的时间内发出警报，需注意的是防火墙比较常见，但是在下载防火墙时要选择正规的网站，并对安装环境进行检查。

3.5 制定有效的网络安全审计跟踪技术

一般而言，对于国家重点部门更需做好安全防护工作，其中在大数据时代如果出现安全问题会引发经济损失，甚至还会对国家的安全性产生威胁，其中要针对性地选择网络安全审计跟踪技术，要由政府加以干预，做好研发，出台相应的规章制度，尤其要将出售他人信息的行为进行打击，对可能出现的各类风险进行防范分析。通过安全审计跟踪技术，及时发现各类数据流，在程序发生错误时要及时地终结交易，对交易进行检测。防火墙可以实现对病毒的筛选，但是其中仍存在不足，而网络安全审计跟踪技术的应用便可以将防火墙的不足之处加以弥补，能够对各类网络行为进行识别。大数据时代下云计算服务诞生，云计算服务改变了传统的存储模式，但是如果云端受到攻击，会影响用户数据的安全性，所以在今天不可仅仅利用防火墙作为主要的防范对策，要选择多样的方式进行组合，将安全等级系数调高。

3.6 完善网络政治安全工作

完善网络政治安全工作时，要做好顶层设计和战略统筹，制定完善的安全战略布局以及政策，并做好宣传与教育，在积极弘扬主旋律的同时实现网络的生态化发展。同时，还要制定关于网络安全的各项规章制度与技术标准，加强自主研发，完善各项体系，推动大数据技术与网络的相互整合，在增强全民网络安全意识的同时减少网络安全事故的发生[9]。

3.7 定期查杀病毒

在大数据时代需做好病毒的查杀工作，完善病毒防御方案，无论是病毒的检测、预防还是清除，都要体现出系统性与全面性。应用电脑时可以在系统中融入杀毒软件，做好定期查杀，避免电脑受到病毒所带来的影响，如果电脑已经受到病毒所带来的侵害，则要选择专业的杀毒程序与软件。杀毒程序软件可以及时地查明病毒的原因，在全方位杀毒当中也能够保证数据信息的安全性。

3.8 增强用户的网络安全意识

正因为用户缺乏网络安全意识，所以在使用计算机时出现诸多问题，为进一步提高计算机使用的安全性，减少各类网络伤害事件的发生，不仅要做到以上几点专业防护，而且还要从用户安全意识入手，提高用户的警惕性，引导用户对安全问题加以重视，在计算机操作中能够避免不正当操作现象的发生。除此之外，在应用信息技术进行金钱往来时，更要提高警惕。换而言之，对于网络监管部门要对群众加以引导，积极宣传关于计算机方面的知识，选择真实案件为人们敲响警钟，或者人们在应用计算机进行数据传输时要对不和谐因素加以分析，如出现防火墙阻拦信息，要及时关闭不良页面，加以重视。

3.9 做好系统组件的更新

因计算机技术属于高效率的发展体系，在大数据时代下为减少安全事故的发生，须进行系统组件的实时更新，如此可有效地满足大容量数据的基本处理需

求。另外，为了有效地缩短软硬件、计算机体系之间的差距，同样要对各类组件展开更新，满足基本的使用需求。承接各类软件的运营商要从自身出发，积极做好优化处理，而且还要及时地查找漏洞，避免软件受到侵害，这也能提高安全属性，为用户的操作带来保障。

4 结语

总之，大数据时代下做好网络计算机安全防护工作至关重要，这个关系到了人们的生活、工作与学习，其中要构建计算机安全网络体系，从不同的角度出发，避免计算机受到病毒、黑客所带来的侵扰，同时还要提高其安全属性，加强对软硬件的更新，实现病毒的查杀，选择各类加密技术与身份验证技术等，如此，能够真正减少网络安全问题的出现。

参考文献

[1] 胡美正.浅析大数据时代的计算机网络安全及防范措施[J].电脑知识与技术,2020,16(36):38-40.
[2] 陆欢荣.云计算环境下的计算机网络安全防范研究[J].网络安全技术与应用,2021(08):76-77.
[3] 齐红.大数据时代下计算机网络安全防范的研究[J].中小企业管理与科技(上旬刊),2021(10):104-106.
[4] 肖承望.中职院校计算机信息网络安全技术和安全防范策略探讨[J].网络安全技术与应用,2021(11):99-100.
[5] 刘雷,董超.大数据时代背景下计算机网络安全防范应用与运行[J].网络安全技术与应用,2019(06):51-53.
[6] 宋人愚.人工智能时代高校计算机网络信息安全问题研究[J].计算机产品与流通,2019(06):209.
[7] 葛小虎.关于计算机网络安全防范中防火墙技术的应用分析[J].网络安全技术与应用,2019(11):21-23.
[8] 吴欣妍,薛峰,刘琦.关于计算机网络通信安全问题分析与防范策略探讨[J].电脑知识与技术,2019,15(28):47-48+55.
[9] 王国庆,陈辉.试谈大数据时代的计算机网络安全及防范措施[J].IT经理世界,2020,23(3):102.

（上接第26页）

时，干扰源释放强度较低的干扰信号，通过观察发现无人机继续沿着设定好的航线飞行至AD线之间的B点处（详情如图4所示），说明该干扰信号并没有对无人机的正常飞行产生影响，当无人机飞行过B点时，开始进行欺骗信号强度的增强，每秒增加1dB，持续时间为10s。无人机仍然按照既定的航线进行飞行作业，不过通过载噪比的数据对比发现这个时候无人机已经接入了欺骗信号，并且在系统内占据主导定位，预设航线数据被影响。这个时候干扰源对无人机进行欺骗信号数据的改变，诱导无人机偏离原本预设的航线向西南方向飞行，并且干扰时间为5s，在这之后可以明显地观察到无人机偏离了原本的航线，说明欺骗干扰试验成功。

3 结论

在本文的论述中以欺骗干扰技术为基础进行了干扰型号模型的而设计，通过民用接收机以及大疆无人机作为实验对象进行可行性验证，结果表明，基于不需要对正确信号压制的情况，就可以成功实现对目标设备的

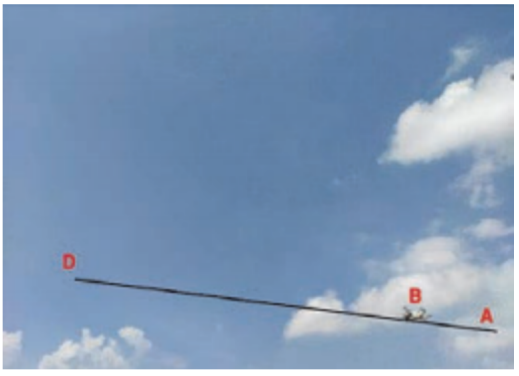

图 4 动态干扰测试中无人机航线的设定

干扰，从而使其偏离原本的航向，具有较高的可行性。

参考文献

[1] 马海宁，潘颜楠，孙志.基于欺骗干扰技术的导航对抗新途径[J].指挥控制与仿真，2021,43(4):67.
[2] 胡洪涛，李正杰，兰竹.基于卫星导航欺骗干扰的无人机诱捕技术[J].电子信息对抗技术，2020,35(2):16-17.
[3] 陈保豪，李任新.基于卫星导航欺骗干扰情况下的无人机管制技术研究[J].信息系统工程，2019(10):156.
[4] 施林，刘伟.基于卫星导航欺骗干扰的无人机管制技术[J].指挥信息系统与技术，2017,8(1):78-79.