2023年网络安全技术论文题目新颖 无线网络安全技术论文(精选5篇)

在日常学习、工作或生活中，大家总少不了接触作文或者范文吧，通过文章可以把我们那些零零散散的思想，聚集在一块。那么我们该如何写一篇较为完美的范文呢？以下是小编为大家收集的优秀范文，欢迎大家分享阅读。

网络安全技术论文题目新颖篇一

摘要无线异构网络能够提高公众网络的覆盖面积以及容量和通信能力，同时异构网络还可以改善公众移动网络的intemet的能力和移动计算能力的现状。因此，无线异构网络技术得到了人们关注，并且无线异构网络拥有广阔的发展前景。本文主要研究无线异构网络的安全技术中的安全路由协议以及接入认证技术和入侵检测技术等关键安全技术。

无线异构网络是网络通信技术迅速发展的佳绩，它可以将各种各类网络进行融合□4g网络就是无线异构网络融合技术重要成果。异构网络融合技术可以提升蜂窝网络的功能，为我国网络通信发展做出了杰出的贡献，打开了我国网络通信的新局面。

1安全路由协议

安全路由是实施异构网络的关键技术，它在异构网络中主要作用就是发现移动的协议点和基站。在过去，路由协议的关注点主要集中在选路以及策略，从而忽略了安全问题。但在在ucan中容易出现的安全问题主要集中在数据转发路径上合法中间节点的鉴定。路由发出的消息中又包含密码的mac□mac能够对经过的路径进行鉴定，这样基站就能够对所有的代理和转发节点的数据流编号进行定位，并且所有的用户都有一个属于基站所给的密码。联合蜂窝接入系统主要

功能就是间断个人主机撤消合法主机，和给以转播功能给为认可的主机，并且它还能够阻止自私节点，但是如果发生了碰撞ucan的防御能力就会下降。有研究者提出一种新路由算法可以有效解决任意碰撞，新路由算法可以优先保护路由机制和路由数据，并且能够对网络信任模型进行高度融合，并且对安全性能进行有效的分析。新算法的主要原理就是：加强对主机发送信息给基站的线路进行规划，规划的线路具有吞吐量高的特点。这就要求对主机邻近的节点的吞吐量进行测量。

对安全路由协议的研究主要是对基站和移动终端的路由安全以及任意2个移动终端间的路由安全进行研究。无线异构网络的路由协议来源于adhoc网络路由协议的扩展，所以在对异构网络路由协议安全性研究应该从adhoc网络路由协议安全着手，所以在进行对无线异构网络进行建设时，通常是直接将部分adhoc安全路由植入到异构网络的安全路由研究中。

2接入认证技术

市场上的认证体系主要是适用于一般式集中网络kerberos和x.509是运用最为广泛的认证体系，并且这两个体系都具有认证机构发放的证书。异构网络的认证系统则是比较灵活多变的，异构网络既有集中网络，同时又包括分散式网络。接入认证是异构网络安全的第一道防线，所以应该加强对那些已经混入网络的恶意节点的控制adhoc与蜂窝融合网络具有三种体系，当蜂窝技术占据主导位置，接入认证的主要工作就是将adhoc中合法的用户安全的接入到蜂窝网络中，当adhoc在融合中占据主导位置，接入认证的主要工作则会发生相应的改变，工作的核心就是让adhoc内部实现安全，蜂窝管理adhoc网络进行安全的传送和控制信息。

接入认证是异构网络安全的第一道防线，所以应该加强对那些已经混入网络的恶意节点的控制。所以在异构网络的认证

系统中应该加强对基站和节点的声誉评价。因为ucan的末端接入网络需要依靠节点的广泛分布和协同工作才能进行正常的运行，在运行中不仅要拒绝恶意节点的接入，同时还要对节点和基站进行正确的评价，保护合法节点免遭恶意节点的影响而被拒绝接入，这样能够有效提升网络资源的利用率。异构网络中声誉机制中心主要是由基站和移动节点担任的，基站在声誉评价中起主要作用，节点对评价进行辅助。同时还可以对节点接入网络时展开预认证，同时网络中的基站以及其他的移动节点可以对节点的踪迹进行追踪，并对节点的恶意行为进行评价。

3入侵检测技术

无线异构网络和有线网络有着天壤之别，因此，有线网络的入侵检测系统在异构网络中不能发挥作用。传统的入侵检测系统主要工作就是对整个网络进行的业务进行监控和分析，但是在异构网络中的移动环境可以为入侵检测提供部分数据，数据主要是无线通信范围内的与直接通信活动有关的局部数据信息，入侵检测系统就根据这不完整的数据对入侵进行检测。这些一般的入侵检测系统不能对入侵进行识别，同时一般入侵识别系统还不能对系统故障进行判断，但是异构系统能够有效解决这些问题。

异构系统入侵系统主要包含两种如期那检测系统，并且均得到了市场的好评。

（1）移动代理技术的分布式入侵检测系统。

(2)adhoc网络分布式入侵检测系统。

移动代理技术的分布式入侵检测系统主要构件是移动代理模块，它的工作原理是，依照有限的移动代理在adhoc中发挥的作用不同，并且将移动代理发送到不同的节点，在节点中实施检测工作□adhoc网络分布式入侵检测系统能够让网络中的

每一个节点都参与到入侵检测工作中，并且每一个节点都拥有入侵检测系统代理，入侵检测系统代理可以作用于异常检测。所以，当某一个节点发送出异常信号时，不同区域的入侵检测系统代理就可以共同协作，展开入侵检测工作。

4节点协作通信

节点协作通信主要工作就是保证节点通信的内容在adhoc网络中能够保密的进行传送，并且保证异构网络中adhoc网络的安全，免受恶意节点和自私节点的入侵。所以在异构网络中的关键安全技术的研究中还要设计出一种激励策略，来阻止恶意节点的攻击和激励自私节点加入到协作中，完成通信内容在传送过程保密。在无线异构网络中的节点写作通信主要有两个方案，一是基于信誉的策略，二是基于市场的策略。

5结论

异构网络在未来网络发展中占据着重要的位置，所以人们不断对异构网络进行研究。异构无线网络融合技术可以实现无线网络和有线网络的高度融合，未来无线移动网络的发展离不开异构网络，异构无线网络将更好的服务人们的生活生产，为人们创造更多的经济价值。

参考文献

作者单位

国网物资有限公司北京市100120

网络安全技术论文题目新颖篇二

通过气象网络安全方面的建设，首先要加强本部门业务科技人员的安全意识，制定规范、严格的流程管理制度和业务流程。做到责任明确，通过网络硬件设备记录详细的网络访问

行为，通过安全审计功能，能及时发现不文明的网络行为。通过定期的组织信息安全方面的培训，对气象部门网络和个人电脑、服务器的关键点进行长期信息收集、分析得出薄弱点和加强防护之处提高网络安全的效率，规避风险。

图1漳州市气象局网络结构图

参考文献

[1]林志雄等。地理知识云服务系统的安全等级保方案设计与安全功能逻辑评估。互联网论文库。

[2]陈进等。浅析信息安全风险与防护策略[j].福建电脑。,27（8）

[3]蒋志田等。电子政务系统安全问题的研究与实践[j].北京邮电大学。,15（13）

网络安全技术论文题目新颖篇三

[摘要]随着现代社会的计算机技术及其应用的不断发展，人们对于网络的应用已经越来越有心得。然而随着这种技术的发展和成熟，计算机对于通信的要求也越来越高。但是，局限于不同的地域对于网络传输能力的差异，在许多情况下，有线通信已经开始渐渐无法满足人们对网络的要求。基于此，在有线网络的基础之上，无线计算机网络通信技术应运而生。无线网络一般具有高移动性、建网容易、管理方便、兼容性好等优点，从而得到了不同领域的广泛应用。然而随着无线网络应用领域的扩大和应用层次的不断深入，无线通信网络本身所蕴含的缺陷也不短的暴露出来，这些漏洞往往会遭到黑客攻击而导致使用者个人信息外泄，甚至对一个的财产等方面也会有一定的影响。网络安全问题日渐成为人们比较关心的一个话题。

[关键词]无线网络漏洞安全

是随着无线网络应用领域的扩大和应用层次的不断深入，无线通信网络本身所蕴含的缺陷也不断的暴露出来，这些漏洞往往会遭到黑客攻击而导致使用者个人信息外泄，甚至对一个的财产等方面也会有一定的影响。无线网络的安全问题正在不断被更多人关注。

一、无线网络中存在的安全隐患

（一）会话拦截以及地址欺骗

在无线环境中，非法用户通过非法侦听等手段获得网络中合法终端的mac地址比有线环境中要容易得多，这些合法的mac地址可以被用来进行恶意攻击。另外，由于ieee802.11没有对ap身份进行认证，非法用户很容易伪装成ap进入网络，并进一步获取合法用户的鉴别身份信息，通过拦截会话实现网络攻击。

（二）无线窃听

在无线网络中所有的通信内容一般都是通过无线信道传送的，任何具有适当无线设备的人均可通过窃听无线信道而获得所需信息。对于无线局域网其通信内容更容易被窃听，因为它们都工作在全球统一公开的工业、科学和医疗频带，虽然无线局域网通信设备的发射功率不是很高，通信距离有限，但实验证明通过高增益天线在其规定的通信距离外仍可有效的窃听。

（三）信息篡改

信息篡改是指攻击者将窃听到的信息进行修改（如删除或替代部分或全部信息）之后再将信息传给原本的接受者，其目的有两种：恶意破坏合法用户的通信内容，阻止合法用户建

立通信链接；将修改的消息传给接收者，企图欺骗接受者相信修改后的消息。信息篡改攻击对物理网络中的信令传输构成很大的威胁。

（四）未经授权使用网络服务

由于无线局域网的开放式访问方式，非法用户可以未经授权而擅自使用网络资源，不仅会占用宝贵的无线信道资源，增加带宽费用，降低合法用户的服务质量，而且未经授权的用户没有遵守运营商提出的服务条款，甚至可能导致法律纠纷。

（五）高级入侵

一旦攻击者进入无线网络，它将成为进一步入侵其他系统的起点。多数企业部署的wlan都在防火墙之后，这样wlan的安全隐患就会成为整个安全系统的漏洞，只要攻破无线网络，就会使整个网络暴露在非法用户面前。

二、对于无线网络安全隐患的对策

基于上述无线网络的安全问题，也为了能保障我们使用无线网络上网时的踏实，相应的无线安全技术也应运而生，这些既是一般包括三大核心：认证性、加密性、完整性，这三大核心贯穿整个防御机制当中，诸如物理地址(mac)过滤、服务区标识符(ssid)匹配、有线对等保密(wep)□端口访问控制技术(ieee802.1x)□wpa(wi-fiprotectedaccess)□ieee802.11i等。而其具体的方法可以罗列如下：

（一)物理地址(mac□过滤

每个无线客户端网卡都由唯一的48位物理地址(mac)标识，可在ap中手动设置一组允许访问的mac地址列表，实现物理地址过滤。这种方法的效率会随着终端数目的增加而降低，而且非法用户通过网络侦听就可获得合法的mac地址表，

而mac地址并不难修改，因而非法用户完全可以盗用合法用户的mac地址来非法接入。因此mac地址过滤并不是一种非常有效的身份认证技术。

（二）加密机制

保密性业务是通过加密技术实现的，加密是一种最基本的安全机制，加密过程如图1所示：当加密密钥不等于解密密钥，即系统中每个用户拥有两个密钥（公开密钥和秘密密钥），则称其为非对称密码系统或公钥密码系统。任何人都可用一个用户的公开密钥将信息加密后传给该用户，只有该用户才能用其秘密密钥解密，其他人因不知道秘密密钥而不能解密。公钥密码算法复杂，因而不适合资源受限的无线通信设备，但由于其不需要通信双方共享任何秘密，在密钥管理方面有很大的优越性。

(三)eee802.11i标准

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，ieee802.11工作组开发了新的安全标准ieee802.11i，并且致力于从长远角度考虑解决ieee802.11无线局域网的安全问题，ieee802.11i标准针对802. 11标准的安全缺陷，进行了如下改进。身份认证，802.11i的安全体系也使用802.1x认证机制，通过无线客户端与radius服务器之间动态协商生成pmk(pairwisemasterkey)，再由无线客户端和ap之间在这个pmk的基础上经过4次握手协商出单播密钥以及通过两次握手协商出组播密钥，每一个无线客户端与ap之间通讯的加密密钥都不相同，而且会定期更新密钥，很大程度上保证了通讯的安全。

（四）身份认证机制

身份认证技术提供通信双方的身份认证，以防身份假冒。它

通过检测证明方拥有什么或知道什么来确认证明方的身份是否合法。密码学中的身份认证主要基于验证明方是否知道某个秘密（如证明方与验证方之间共享的秘密密钥，或证明方自己的私有密钥），基于共享秘密的身份认证方案建立在运算简单的单密钥密码算法和杂凑函数基础上，适合无线通信网络中的身份认证。

(五)ssid匹配

无线客户端必需与无线访问点ap设置的ssid相同，才能访问ap;如果设置的ssid与ap的ssid不同，那么ap将拒绝它通过接入上网。利用ssid设置，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能的问题。可以通过设置隐藏接入点(ap)及ssid区域的划分和权限控制来达到保密的目的，因此可以认为ssid是一个简单的口令，通过提供口令认证机制，实现一定的安全。

三、结束语

现代社会对于无线网络的使用已经蔓延到了我们生活的各个领域，不同领域对于这种无线网络的需求和要求也不断的提高，加上现代社会竞争压力不断的增大，无线网络作为一种信息交流平台具有很强的商业和企业价值，如果在这一个方面产生问题的话，会对我们的生活乃至是一个企业的存亡都有很大的关系，可是作为一个信息交流的媒介它又必然也存在许多的漏洞，这种漏洞会造成信息流失、商业价值贬值、个人隐私泄露等不同程度的损害，所以对于无线网络的安全问题的研究刻不容缓。

参考文献

[1]谢俊汉。浅析计算机无线网络技术及其应用[j]□中国教育技术装备，2007.

[2]刘剑。无线网通信原理与应用[m]□清华大学出版社，2002，11，01.

[3]iimgeier(美)。无线局域网[m]□人民邮电出版社，2001，04，01.

[4]卡什□cache□j.□□无线网络安全。北京：机械工业出版社，2012.3.

[5]池水明，孙斌。无线网络安全风险及防范技术刍议。信息网络安全，2012.3.

网络安全技术论文题目新颖篇四

无线互联网中，应用主体互联网优势比较明显，存在较多路由器种类。比方说，各个科室间有效连接无线网络，还能实现实时监控流量等优点，这就对互联网信息可靠性与安全性提出更大保障与更高要求[3]。以此为前提，无线互联网还可以对外来未知信息进行有效阻断，以将其安全作用充分发挥出来。

3.2对无线数据加密技术作用进行充分发挥

在实际应用期间，校园无线网络必须对很多保密性资料进行传输，在实际传输期间，必须对病毒气侵入进行有效防范，所以，在选择无线互联网环节，应该对加密技术进行选择，以加密重要的资料，研究隐藏信息技术，采用这一加密技术对无线数据可靠性与安全性进行不断提升。除此之外，在加密数据期间，数据信息收发主体还应该隐藏资料，保证其数据可靠性与安全性得以实现。

3.3对安全mac协议合理应用

无线传感器网络的形成和发展与传统网络形式有一定的差异和区别，它有自身发展优势和特点，比如传统网络形式一般是利用动态路由技术和移动网络技术为客户提供更好网络的服务。随着近些年无线通信技术与电子器件技术的迅猛发展，使多功能、低成本与低功耗的无线传感器应用与开发变成可能。这些微型传感器一般由数据处理部件、传感部件以及通信部件共同组成[4]。就当前情况而言，仅仅考虑有效、公平应用信道是多数无线传感器互联网的通病，该现象极易攻击到无线传感器互联网链路层，基于该现状，无线传感器网络mac安全体制可以对该问题进行有效解决，从而在很大程度上提升无线传感器互联网本身的安全性能，确保其能够更高效的运行及应用[5]。

3.4不断加强网络安全管理力度

实际应用环节，首先应该不断加强互联网安全管理的思想教育，同时严格遵循该制度。因此应该选择互联网使用体制和控制方式，不断提高技术维护人员的综合素质，从而是无线互联网实际安全应用水平得到不断提升[6]。除此之外，为对其技术防御意识进行不断提升，还必须培训相关技术工作者，对其防范意识予以不断提升；其次是应该对网络信息安全人才进行全面培养，在对校园无线网络进行应用过程中，安全运行互联网非常关键[7]。所以，应该不断提升无线互联网技术工作者的技术能力，以此使互联网信息安全运行得到不断提升。

网络安全技术论文题目新颖篇五

多媒体与多媒体技术论文，多媒体和多媒体技术是两个不同的概念，分清其定义和特点，对探究多媒体技术是必不可缺的。

多媒体与多媒体技术论文【1】

摘要：我们通常所说的“多媒体”，大多是指处理和应用多媒体的一些技术，而不是说多媒体信息本身，将“多媒体”和“多媒体技术”当作了同义词。

关键词：多媒体多媒体技术定义特点

一、定义

1、多媒体

对多媒体的定义目前还没有统一的标准，但通过对各种定义的分析，笔者认为可以这样进行定义：多媒体是融合两种或两种以上的媒体的一种人机交互式信息交流和传播媒体。在这个定义中我们应明确以下几点：

(1)从功能上看，多媒体是信息交流和传播的媒体，与电视、报纸等所具有的传媒功能相当。

(2)从运行程序上看，多媒体是人与机器的交互。机器主要是指计算机，抑或是有微处理器控制的其他终端设备。在运行程序中，多媒体和计算机或其他终端设备实现了“交互”，对信息进行处理，这是其他媒体所不能完全具有的。

(3)从处理形式上看，多媒体信息都以数字形式而呈现，不是以模拟信号的形式进行存储和传输。

(4)从构成种类上看，凡文字、图片、声音、动画、图形等只要是两种以上的媒体进行整合便构成了多媒体。

2、多媒体技术

多媒体技术实质上就是运用多媒体的技术，通过采用计算机技术对文字、图片、动画等媒体进行整合，让它构建起逻辑连接，并能对它们进行获取、编码、处理、存储和展示。

由于多媒体依靠计算机或其他终端进行信息处理的的技术，使它具有了以下特点：

(1)信息载体的多样性

多媒体使用的载体其实就是计算机，这就决定了它的多样性。多媒体是把计算机所能处理的信息空间进行拓展，不再单纯的局限于数值、文本。计算机所带来的信息，并不能被人的大脑所全部接受，只有通过转换后方能达到更高的接受水平。多媒体其实就是将计算机处理的信息更多样化、更直观化地呈现出来。

(2)信息载体的集成性

由于多媒体是对文、图、声、像进行综合处理的技术，使之具有了集成性，集成性也可以成为综合性，主要表现在信息的集成和设备的集成两个方面。对信息集成而言，集成是对多种信息进行整合的过程，将多个单一的媒体信息进行组织后，使之以并生的形式呈现。

如教学中常用的幻灯片，同时能进行文字和图片的展示，其实就是对文字信息和图片信息进行整合，让文字和图片同时呈现在接受者面前。对设备集成而言，硬件设备需要能进行高速运转及并行的cpu系统，存储设备需要适合媒体的输入与输出;软件设备需要保证对媒体信息进行系统管理和应用。

(3)信息载体的交互性

信息媒体的交互性是多媒体技术的标志特征，这一特性使人们对信息的获取和使用由被动转向主动，交互性让信息更加的直观、形象，使信息的保留时间得到延长，更利于获取和使用。

交互性时多媒体技术区别于其他技术的特点，特别是在教学

中，人机回话使得多媒体的功能得到了充分的体现。

二、多媒体的构成

由于多媒体是所处理的对象主要是生意和图像信息，而由声音和图像信息的特点所决定，多媒体的构成应包括：

1、计算机：包括个人的计算机或是工作站。

2、视听接口：声卡、视频卡、图像处理卡和多功能处理卡等。

3、输入设备：话筒、摄影机、扫描仪等。

4、输出设备：耳机、显示器、合成器等。

5、存储设备：光盘□u盘、硬盘等。

6、应用软件：系统软件(windows等)、开发工具包括创作软件工具和编辑工具，如编辑制作的工具powertpoint和photoshop等。应用软件是多媒体硬件平台和创作工具上开发的应用工具，如演示软件、游戏等。

三、多媒体技术简介

多媒体依托于计算机而成为了一项崭新的技术，其应用领域逐渐广泛，先做以下多媒体技术的简要介绍：

1、音频、视频处理

这是多媒体计算机系统中常见的表现形式，多媒体技术通过计算机或者其他处理系统，对音频和视频进行处理，以直观的方式呈现。

2、数据处理

在多媒体计算机的处理过程中，传输和处理文、图、声、像等信息需要占用大量的空间，这就需要对信息进行压缩和解压，而这也正是多媒体运行系统中的关键，只有对信息能进行高效的压缩和解压，方能为信息的处理带来便捷化。

3、软件开发

多媒体的使用需要软件进行支撑，这也促进了软件技术的发展。在多媒体操作系统上有很多的开发工具，
如flash□3dstudio等，他们为使用者提供了对图像、声音、视频等多种媒体进行便捷、制作、合成的功能。

4、通信技术

多媒体技术最主要的目的就是要加速和方便信息的交流，因此，多媒体技术书通信技术的关键技术之一。多媒体通信技术是通信技术、计算机技术和电视技术的相互渗透、相互影响的结果。目前，随着信息技术的发展，电子通信基本上走上了数字化道路，这也正是多媒体作用于通信技术的’表现。

5、超文本和超媒体

文档为doc格式