DOI 编码：10.13646/j.cnki.42-1395/u.2020.05.027

基于智慧船闸的网络安全策略

阚国春

（江苏省施桥船闸管理所，江苏 扬州 225000）

摘　要：目前，信息化技术获得跨越式发展，越来越多的企事业单位都认识到依托先进的 IT 技术构建自身的业务和运营平台将极大地提升运营效率。信息化运行尤其依赖于计算机系统，而这一系统又尤其依赖于互联网。现如今，持续扩大的互联网规模，伴随发展的还有日益复杂的互联网结构，为了更好地运行计算机应用系统和计算机网络，网络安全问题需要提高标准。本文以施桥船闸为例，研究探索在践行智慧船闸时，作为网络管理人员应该如何应对日益复杂的网络环境，思考如何将网络变得更加安全可靠。

关键词：智慧船闸；网络系统；安全策略

中图分类号：U641　　**文献标识码：**A　　**文章编号：**1006—7973（2020）05-0067-03

1 前言

智慧船闸主要是指依靠先进的控制技术、通信技术、传感器技术等，将潮流的 AI 技术、大数据技术、5G 及云技术等技术有效集成，充分应用于船闸通航管理服务中，在船舶过闸时发挥其高效、准确作用的综合管理控制系统，利用这些先进的技术提高船闸的运行效率，减少船民的过闸等待时间和经济成本，从而为船员提供更加周到的服务。

施桥船闸管理所位于古城扬州市南郊的施桥镇，管理着三座大型现代化船闸，是苏北运河过长江向北十个梯级过船枢纽的第一道船闸，素有苏北运河“南大门”之称。施桥船闸下游距长江 6.5 公里，上游距邵伯船闸 23.5 公里，年双向设计通过能力为 1.5 亿吨，船闸常年有 10 多个省市的船舶通过，是煤炭、建材水运的重要通道，2016 年以来，因黄沙等建材运量增多等原因，施桥船闸已经成为苏北运河最为繁忙的船闸，2017 年通过量首超 3 亿吨达 3.29 亿吨，创下全国内河船闸之最，全年有 42 次日通过量超百万吨。

近年来，施桥船闸大力推动智慧船闸建设，创新管理模式，提高船闸通过能力，优化工作流程，提高过闸效率，在服务地方经济和国民经济发展中日益发挥着十分重要的作用。但随着网络的产生和应用，网络安全问题也随之出现。如何加强网络安全，确保生产高效运行，每个计算机用户，特别是企事业单位网络用户，安全措施必须足够。

2 研究背景

网络安全策略的实施是一项系统工程，它涉及许多方面。因此不仅要对平时的外部网络威胁多加考虑，而且还要足够重视网络管理和内部网络所存在的安全隐患，不能孤立地看待任何一个安全隐患和安全措施。因为有可能会呈现出多方面的安全隐患爆发途径，因此所采取的安全措施都必须是相互关联的。比如黑客攻击和病毒入侵等非常典型的事件，全是借助网络实施的攻击行为，而且几乎每时每刻都在发生，遍及全球。除此之外，比如非法截取和更改用户邮件，用户的非法操作和访问，恶意软件的攻击和入侵等都是普遍存在的安全事实。

目前病毒感染不再是防范的唯一对象，还要防范以网络为载体的非法访问、攻击和入侵，将安全隐患在单位网络中的发生划分为外网和内网两部分，很多情况下内部网络安全威胁要远远大于外部网络，内部实施病毒入侵和攻击更加容易，针对这些安全问题，所实施的安全策略可以通过防护病毒网络版系统的专业安装来执行，在此过程中还要对内部网络安全管理要持续提升强度和质量，对于系统本身安全措施和防火墙过滤策略都要配置好，对于系统安全补丁要第一时间安装，有条件的还可以在外网、内网中安装 IPS 系统、网络嗅探器、网络扫描检测、IDS，还可以考虑将网络安全隔离系统给予一定的配置，对内、外网络进行安全审查；安全管理内部网络要持续加强，严格实行“最小权限”原则，恰当的用户权限要在各用户间配置好；同时对一些敏感数据进行加密保护，对数据还可以进行数字签名措施；根据单位实际需要配置好相应的数据策略，并按策略认真执行。

3 船闸网络安全需求及隐患

一般单位网络普遍应用数据库、电子邮件、HTTP、

续的成功脱浅奠定了基础。

5.4 科学决策实施救助

搁浅遇险船受现场风流的影响，船首向不断变化，专业救助船要科学决策，选择向上风方向，变化救助船首向的方式，实施脱浅救助作业。并在脱浅后，专业救助船合理使用车、舵控制拖力、船位和船速，避免搁浅遇险船由于惯性冲撞附近灯浮事故的发生。

6 结束语

海上险情千变万化，同样的险情性质，不同时间，不同海域发生的险情，应急处置方式方法也不尽相同。这就要求专业救助人员要加强救助案例的分析研究和经验总结。本文通过对搁浅遇险船脱浅救助拖力的计算，实施快速有效脱浅救助经验总结，为今后专业救助船在处置此类险情时提供参考。

FTP、TCP/IP 等这些常见的标准和技术，将丰富的通信形式作为技术依托，实现广域连接。在飞速的信息流中，信息的处理、存储、传输等都关系到行业内部消息。所以加以保护有关的信息资源是非常必要的，还要管理和控制服务资源。

3.1 施桥船闸网络安全需求

施桥船闸是有着 100 多名职工的中小型网络单位，主要是依靠船闸智能调度系统服务水运事业。单位网络主要分为内网与外网，网内现有计算机约 100 余台，服务器的操作系统包含 Windows Server 2003 和 Windows Server 2008, 客户机的操作系统是含有 Windows XP、Windows 7、Windows 10，客户机在工作组的模式下运行。单位对网络的依赖性很强，主要业务都要涉及互联网以及内部网络。随着智慧交通体系的建设，智慧船闸也已成为当下发展的主流趋势，因此构建健全的网络安全体系以满足智慧船闸对网络安全的需求是重中之重。

3.2 施桥船闸网络安全隐患

网络内部和外部都会受到网络入侵，办公信息安全和网络系统都会因为网络攻击而受到危害，一般可以将危害具体总结为：

（1）借助木马程序来使得非法用户对计算机系统进行控制，将计算机上的资料删除或者任意复制。

（2）设置的共享权限和口令策略不够安全，计算机上的资料可以由其他用户借助网络完成复制。

（3）保密文件可以由病毒自行散发，比如说这种 SirCam 病毒。这种病毒会将电脑中的 Word Excel 等资料以邮件附件形式向其他邮件传送，甚至有美国联邦调查局 (FBI) 的一些资料也以这种方式发送出去。

（4）对于网络中明文传输的数据可以借助网络侦听 (Sniff) 实现截获，比如像 FTP、Telnet、电子邮件等资料在利用简单编码或者明文进行传输过程中，存在被非法用户半路截获的可能，从而导致泄漏资料。

（5）中断服务。对于办公网络来讲，就是以网络为载体实现有关办公流程的网络化和自动化，现如今主要应用的办公网络是办公自动化系统 (OA)，假设该系统受到攻击，系统很有可能无法提供服务，造成办公自动化中断，使得办公效率下降，甚至工作流程更为混乱。

3.3 施桥船闸网络安全需求分析

通过了解施桥船闸的需求与现状，为实现网络安全建设和改造升级网络系统，运行网络系统的稳定性予以提高，保证单位各类信息系统的安全性。对于客户端的计算机准备采用安全手段来进行保护，将用户在客户端计算机中的文件操作和目录操作进行记录，旨在有手段实现单位对计算机使用情况的实时查看和追踪，旨在避免外来计算机入侵单位网络系统。借助改造优化网络结构，使得管理者能够实时监控和管理软件安装、登录用户权限、网络中服务器等方面应用。因此需要：

（1）构建良好的环境确保单位物理设备的安全；

（2）进行科学有效的 VLAN 划分，内网安全实时控制；

（3）安装防火墙体系；

（4）组建入侵检测系统；

（5）安装防病毒服务器；

（6）加强对网络资源的管理；

（7）增加访问控制策略；

（8）增加信息加密策略。

4 施桥船闸网络安全策略

4.1 访问控制策略

非法访问予以有效避免是访问控制的基本目标，可以实现用户安全控制服务器和关键网络。现如今应用非常普遍的网络访问控制设备就是防火墙，这一设备借助端口号、IP 地址等实施设置和控制有关的安全代理等方法，完成隔离外部网络和内部被保护网络。

单位网络在安全规则方面能够对一段网络、一组主机、单独主机，以网络协议为基础完成基本的设置，完成有关的安全规则编辑；完成安全规则基于网络通讯接口进行设置，仅仅放开其中部分服务端口，以服务于单位保护对象；可以按照具体时间来完成设置，旨在将访问控制顺利实现；安全规则基于网络服务进行设置。

可使用带行为管理的防火墙或者设置代理服务器（如 SQUID）进行行为管理，方便有效地对单位内部局域网进行监管与控制。

4.2 信息加密策略

对于网内的控制信息、口令、文件资料、数据借助信息加密起到保护目的，同时还对传输的网络数据加以保护。密钥网络加密中是需要的，密匙通常指生活、生产过程中各种加密技术的使用，可以高效地监管企事业机密和个人资料，管理密钥的有关行为称之为密钥管理，比如破解、解密、加密等行为都属于密钥管理。

端点加密、节点加密、链路加密是常用的网络加密的三种方法。对于网络节点中的链路信息进行保护是链路加密主要目的；对于目的节点和源节点之间的传输链路提供保护是节点加密的目的；对于目的端用户和源端用户有关数据提供保护是端端加密的目的。

（1）链路加密。可以将其定义为在线加密，任何消息的加密操作都需要在传输之前，对于接收到的每一个节点信息都需要解密，对于消息在下一个链路中再完成加密，进行信息传输。一直到最终的目的地，中间要进行多重的加密、解密操作，确保数据传输安全。

（2）节点加密。要求以明文形式来传输路由信息和报头，这样就能对如何在中间节点处理消息的信息进行获取，大致一致于链路加密和其他信息加密形式。在网络节点处，节点加密是禁止明文形式出现的，对于实现收到的信息解密，之

DOI 编码：10.13646/j.cnki.42-1395/u.2020.05.028

航标运行状态模式识别和数值预测

陈麒龙[1]，陆一军[2]

（1. 中国人民大学，北京 100872；2. 交通运输部东海航海保障中心，上海 200086）

摘　要：针对航标运行状态模式识别依赖经验阈值的现状，为检验经验阈值是否具有普适性，提出基于概率的阈值模式识别效率度量算法。实验结果表明：该算法能准确度量阈值的模式识别效率；经检验，经验阈值不具备普适性。因而，提出基于概率的模式识别模型。实验结果表明：以概率作为阈值具有普适性，该模型能准确识别频繁模式和异常模式，且性能更好。为实现数值预测，提出基于概率密度的加权平均算法。实验结果表明：该算法的预测精度较高。本文为航标运行状态模式识别和数值预测提出了新的解决方案。

关键词：水路运输；航标；概率；模式识别；数值预测

中图分类号：U644.8　　**文献标识码**：A　　**文章编号**：1006—7973（2020）05-0069-05

航标遥测数据是反映航标运行状态的数值信息，包括：数据采集时间（Time）、电压（Voltage）、电流（Current）、航标位置（Longitude、Latitude）、离位距离（Distance）。频繁模式表示航标的“常态”，异常模式表示航标的“非常态”。对频繁模式和异常模式的识别，传统方法是依据经验阈值进行分类，存在主观臆断的问题。对航标运行状态的数值预测，目前仍处于研究阶段。如何检验经验阈值是否具有普适性，如何实现航标运行状态的数值预测，是亟待解决的问题。

对数据的频繁模式和异常模式的模式识别，已有不少算法和模型，如：基于相关性度量算法、基于频繁子树算法、基于最大熵隐马尔科夫模型，以及基于统计特征的支持向量机[1-4]。移动对象位置预测的模型有：马尔科夫模型、高斯混合模型、卷积神经网络模型[5-7]。核密度估计（kernel density estimation，KDE）是一种估计数据的概率密度函数（probability density function，PDF）的算法，利用概率密度函数可以计算出给定数值区间的概率。概率可以用来度量经验阈值的模式识别效率，以此来检验经验阈值是否有效，判定经验阈值是否具有普适性。概率反映随机事件发生的可能性，是客观的，以概率作为阈值进行分类，就是将“大概率”的数据作为“常态”，将“小概率”的数据作为“非常态”，从而使阈值成

后再加密传输，期间要采用不同的密钥。对于网络数据传输安全，节点加密效果非常好，但是攻击者对于通信业务的分析采用节点解密形式予以防范却是存在缺陷的。

（3）端端加密。可以将其定义为包加密或者脱线加密，从源点到终点，在传输数据过程中允许以密文形式存在。在到达终点之前，不进行端端加密消息的解密，主要就是由于整个传输过程中，这些消息均受到保护。通常，在对敏感信息进行传输过程中必须应用端端加密形式。

最有效的网络安全技术之一就是密码技术。依托网络进行加密操作，对于非授权用户的入网或者搭线窃听可以有效地防止，这也是一种对恶意软件进行防范的有效措施。

4.3 数据备份策略

施桥船闸目前对信息化的依赖比较高，服务器及数据的稳定性被给予很高的要求，实现这样的目的，除了采购质量良好的硬件设施外，还可以有效地利用私有云实现信息备份和灾难冗余。对于需要高度可靠性的用户，这样的方式可以使文件信息的安全有保障，正常情况本机存储，私有云自动备份，当工作设备的系统出现故障时，备份设备可以随时异地提供数据读取，保证单位整体的正常运转。同时使用 UPS 对重要设备进行不间断的供电，保证硬件设施的良好运行。

5 结语

近几年，互联网技术获得跨越式发展，在这一过程中伴随而生的巨大问题就是网络安全问题。这是一个普遍存在、覆盖面广的复杂性问题，同时还会涉及到违法犯罪等活动。而在涉及到以下简单的网络安全问题时，仅仅确保无关人员无法完成读取信息，或者不能对传输的信息进行修改。网络安全问题中，部分对象无权使用网络，但是却试图借助一些软件来实现远程服务，窃取一些信息。对于合法消息重播和截获问题也是安全性处理的对象。

本文从建设智慧船闸角度对于解决基础网络设施安全进行了描述，旨在为单位提供信息的完整性、认证性、保密性的保护机制，避免网络系统、数据、服务遭到破坏或者侵扰。现在较为普遍应用的方法有加密技术、认证技术、防火墙等，由于越来越大的运行规模，使得单位网络涉及的安全性问题呈现复杂化特征。因此，维护网络安全将是一件关键任务。在此过程中要对安全因素综合考虑，将有关的安全防范技术进行相互结合，采取科学有效的安全防范措施，保证网络安全。

参考文献：

[1] 王加雪，钱江 . 智慧船闸 [M]. 东南大学出版社 ,2018

[2] [美] 本・斯派维 乔伊・爱彻利维亚 . Hadoop 安全大数据平台的隐私保护 [M]. 人民邮电出版社，2017

[3] 刘化君 . 网络安全与管理 [M]. 电子工业出版社 ,2019.

[4]（美）Saadat Malik 网络安全原理与实践 [M]. 人民邮电出版社 ,2019.