大数据的网络安全态势感知技术分析

蔡波[1]　邓飞[2]　杨露平[3]

（电子科技大学成都学院　计算机学院　四川成都　611731；四川天府新区万安中学　四川成都　610213）

摘要：随着经济、社会快速的发展，科学技术的发展和进步，网络在人类的日常工作及信息生活中扮演着越来越重要的角色，人们的学习、生活以及接触到的一切衣食住行等各方面的信息都几乎离不开各种网络技术，以及经商和贸易交流需要使用的商务网络、学习及培训交流需要用到的知识网络、工作以及办公场所需要使用的信息网络等等，网络技术现在几乎是已经被渗透到了我们生活的各个方面，但也正是因为随着各种网络技术的高速发展所带来的诸多方面的方便，同时也伴随着一系列的网络安全问题，使得人们对网络技术既爱又恨。在这种情况下，科研工作者们一直在进行着技术革新，希望能开发出一种能有效地解决网络安全问题的安全、可靠、快速的防御体系。基于此，文章针对基于大数据的安全态势感知技术，提出了基于大数据网络的安全态势感知技术。

关键词：大数据应用；信息网络及安全系统；网络技术应用

The network security situational awareness technology analysis of big data

CAI Bo　Deng Fei　Yang Luping

（School of Computer Science, Chengdu University, University of ESTC Chengdu, Sichuan 611731;
Wan'an Middle School, Tianfu New District, Sichuan Chengdu 610213）

Abstract: With the rapid development of economy and society, The development and progress of science and technology, The Internet plays an increasingly important role in human daily work and information life, People's study, life and all the food, clothing, shelter, transportation and other aspects of information are almost inseparable from a variety of network technology, As well as business network for business and trade exchanges, knowledge network for learning and training exchanges, information network for work and office space, Network technology has now been penetrated into almost every aspect of our lives, But it is also precisely because of the convenience brought by the rapid development of various network technologies, Also accompanied by a series of cyber security issues, It makes people both love and hate the network technology. In this case, researchers have been carrying out technological innovation, hoping to develop a safe, reliable and fast defense system that can effectively solve the problem of network security. Based on this, this paper puts forward the security situational awareness technology based on big data network for the security situational awareness technology based on big data.

Key words: big data application; information network and security system; network technology application

近年来，互联网的应用范围迅速扩大，应用范围不断扩大，在科技、经济、社会等各个方面都得到了广泛的应用。随着网络的普及，各种安全漏洞也随之出现，比如木马病毒、蠕虫病毒、黑客入侵等等，以及各种新的病毒入侵，比如僵尸网络、代码注入等等。目前常见的安全防范系统都是单一的，单一的防护手段无法提供有效的帮助，常常会导致大量的报警信息和虚假的警报，导致安全信息的有效性降低，导致相关人员无法及时采取有效的防范措施。因此，通过对事件进行智能的分析与综合的安全管理，将各个安全部件整合在一起，形成一个高度协同的、无缝的安全系统，是目前网络安全领域的一个重要研究方向。在此基础上，提出了一种基于大数据的网络安全态势感知技术。通过这种方法，可以拓宽网络的安全视野，为网络安全的智能分析和处理新的安全威胁，解决当前网络安全战略的“瓶颈”，为网络安全态势的认识和预警开辟了一条崭新的道路。

1.常见的网络安全问题

1.1 信息泄露

随着信息技术的发展，人们会因为自身需要在很多软件上进行实名认证，而在这个过程中，不可避免的会将自己的个人信息上传到相应的认证平台上，但网络技术的监管也是有缺陷的，当所有的网络平台都连接在一起的时候，这些人的个人信息就会被曝光，而这些人往往会为了自己的利益而窃取别人的资料。比如 QQ 被窃、身份证号码被别人窃取、银行卡密码泄露等。而且，一旦公司的信息被泄露，那么就会影响到公司的未来，如果不能及时处理好，那么公司就会倒闭，甚至会影响到公司的领导。因此，泄密的安全性问题，无疑会造成很大的影响。

1.2 计算机被病毒侵入

电脑病毒可以造成电脑系统的瘫痪，造成电脑程序的紊乱，造成资料的大量损坏，从而降低网路的利用率，进而影响工作的满意度。当电脑病毒入侵时，若没有足够的专业知识，无法及时处理，就会造成大量的电脑故障、文件丢失等问题。

1.3 个人失误

由于人们对网络的认识不足，在使用密码和程序时会出现一些差错，甚至会因为用户的帐号与别人的网络产生错误，从而造成用户的个人信息外泄、程序不规范等问题。

1.4 黑客入侵

非法入侵的黑客经常会企图入侵他人的帐号、窃取资料、破坏程式及系统，严重地损害网路的整体效能与完整性。网络软件并不是十全十美的，因为它本身就有一定的质量问题，而这些问题也是导致网络安全问题的根源,比如工作人员在自己的电脑上安装了“后门”，一旦被发现，就会导致软件瘫痪，造成无法挽回的后果。

2.网络安全态势感知

2.1 态势系统感知基本概念

态势感知系统的一个重要概念，是在现代军事领域中被正式提出的，它涵盖了三大理论层面，即战略感知、对战争态势的理解、对战争态势的理解、对战争态势的预测。并且会随着网络的逐步崛起而逐步提升到“CSA）。目的是实时获取、理解、显示分析和可延展的主要安全技术因素的数据，这些数据可以快速地导致未来的网络形势发生的显著改变，并据此进行相应的分析和应对措施。

2.2 网络态势安全的风险感知机制分析

随着中国计算机网络和其它电子和通讯技术领域信息化的快速发展，网络工程所面对的主要网络威胁越来越多，网络威胁的范围也越来越大，从多个角度分析的各种主要网络环境态势安全的潜在主要威胁风险因素和网络潜在的安全和危害的危险程度也在不断提高，网络病毒、恶意 Do S/DDoS 网络攻击事件，对国家信息和安全网络造成的潜在威胁和受到威胁的人数也在不断增长。同时，由于网络的安全问题，如网络恶意的黑客攻击等，也在不断地朝着多分

布、规模化、复杂化的方向发展。如果单纯依靠防火墙、入侵检测、防蠕虫、访问控制防火墙等传统的检测和防御技术，已经无法满足整体网络的整体安全性能要求。因此，对目前的网络运行和可能存在的各种威胁，并及时有效地发现和处理各种网络安全异常和异常攻击。实时、准确地了解和掌握当前网络的总体安全性能保护情况，将以前的事后预防、事后自动分析和处理的网络安全问题，转变为事前实时分析、预警和风险预测。通过这种方式，可以减少整个网络的整体安全保护和整体的技术保护和协调。

2.3 网络环境安全与态势安全感知分析

系统网络生态安全与态势感知评估体系的主要组成：数据采集、特征提取、态势感知评估、安全预警四大模块。（1）数据源的获取，是指在一个网站的现有网络中，或者在当前的网络状况下，由服务器收集和抽取数据，其中，服务器提供了一个网站的安全日志、漏洞数据库、恶意代码数据库等资源，并对不同的网站进行了综合的、综合的、完整的数据库。（2）特征提取是指在采集到大量的有用数据后，对其中最有价值的数据进行预处理，从而为后续的工作打下基础。在网络和安全与态势信息感知分析的基础上，数据的收集、分析和抽取是数据处理的基础。（3）态势分析与评价态势关联评价方法其基本原则是：利用计算机技术，对不同的相关识别事件进行多个数据的交叉融合，从时间、空间、协议等多个方面进行多维的关联与识别。简而言之，就是要根据现有的数据和信息，对当前发生的事故进行风险评估，判断事故的危险程度。（4）安全警告：经过上述步骤，提取了大量的网络状态信息，然后按照一定的准则，对当前的网络状况和未来的网络状况做出评价和预测，并做出相应的分析报告，并对其进行安全状态的处理。

3.大数据融合技术背景环境下的网络与安全态势感知技术

3.1 网络安全数据信息的挖掘技术

利用数据挖掘技术，可以有效地解决目前网络信息资源共享和管理中遇到的各类关键技术问题。我们必须在最短的时间内，使网络信息技术平台能够最大限度地整合和使用已有的高广域、异机构化的信息，使网络能够动态、快速、实时地更新这些新的危险网络的攻击响应信息、攻击响应模式等信息，使整个网络的态势安全响应和安全威胁响应的技术要素信息得到快速的动态跟踪和动态跟踪。这为未来的大规模网络安全态势监控与预测、预警等领域的发展，提供了一个较为客观、全面、可靠的基础资料，保证了我们在对网络态势安全的认识和监控管理的整个科学进程中，不会有任何疏忽或潜在的危险因素，从而对威胁进行更加准确、有效的预测。

3.2 大数据背景环境下的网络安全与态势信息感知系统分析模型中的构建

科学地建立数学分析模型的架构，为有效地分析网络环境和态势管理感知分析系统提供了必要的保证，而感知数据分析系统在分析和预测网络安全中所起到的作用，都是建立在大数据基础上的。所以，在大数据时代的背景下，数据分析系统必须具备足够的能力，才能在一定程度上解决网络安全问题的问题，并在一定程度上解决了这个问题。

3.3 大数据的背景支持下基于网络和安全的态势感知系统中的大数据可视化分析与计算应用技术研究

数据收集与分析系统技术是一种以网络为基础，能够准确、及时、高效地处理和控制分布式、海量的分布式信息资源数据的收集和控制的技术关键，也是在当今互联网大数据应用的新背景环境下有效实现构建基于网络上的分布式安全监控、实时态势跟踪分析及感知智能决策系统应用中的又一重要网络分析技术手段。首先，根据系统对网络和大数据安全技术的需求，对可能危害到网络运行和网络安全的因素和因素进行了初步的分析、筛选、汇总、分析和处理。针对目前的复杂系统环境，如网络性能、系统安全性、实时情况探测与感知技术等，以及对大量离线数据进行分析、计算的时间等方面的需求，本文在离线实时数据和实时读取、写入的基础上，提出了离线实时数据读取与写入的技术架构，并对其进行了深入的研究和应用。该技术可以逐步地应用于分布式的数据存储技术，它可以根据实时的动态变化来调整存储的容量，从而实现对离线数据的实时读取和写入，从而使其与传统的离线实时数据以及计算与分析的结果相分离。同时，使用者可以方便地使用 DStream 的界面进行离线数据读取和写入。

4.网络安全的组成部分

4.1 系统安全

为了保障网络的安全，必须确保各类数据处理设备以及各类传输系统的安全、可靠地工作。一般地，其重点是要确保系统的安全和正常工作，防止系统部件的突然故障，给系统的存储、处理功能和各种信息系统带来巨大的损害和潜在的损害。防止因电磁元件的泄漏，造成信息外泄、干扰等。

4.2 网络的安全

在网络环境中，信息的传递是安全的。主要内容有：用户密码识别、访问权限和控制、访问权限、访问方式和控制、安全审核、计算机病毒和控制、数据加密等。

4.3 信息传播安全

在网络平台载体上存储的网络信息 3 W 所进行的网络传播行为的技术安全性，是指在网络中对信息进行的信息发布和相关的结果和处理技术的整个技术安全，其中包括对在线信息的过滤和处理。事实上，这是要集中精力或集中于如何预防和有效地通过公众网络或非法、有害信息来源传播各种有害信息的方法或方法，以及它们的传播过程和可能造成的其它所有有害后果。在网络媒体上进行信息内容传送时，信息的安全性应当着重于对其相对保密性、真实性和数据完整性的严格保护。为了防止黑客利用各种安全防护漏洞进行各种攻击，如盗窃、冒充、诈骗等，这些技术的实质就是为了维护合法使用者的合法权益和合法的隐私权。

5.互联网大数据应用的国家网络和安全环境态势监测感知评价技术研究的主要意义

大数据网络与网络安全管理系统是通过统一和部署，在全国各个数据中心安装了多个监控和报警网络节点，能够实现全天候、动态、实时地监视整个互联网用户的信息，并对各种可能存在的黑客攻击和网络行为进行实时监控并预警，对覆盖广大网络用户群体范围的大数据网络管理与应用安全与管理将做到全面及规模化防护。目前，以大数据为基础，建立以大数据为基础的安全感知与保护感知技术，是目前较为成熟、切实可行的新技术。我们依然坚信，大数据将会给我们的国家带来更多的新科技。

结束语：

综上所述，基于大数据的网络安全态势感知技术是解决网络安全问题的重要手段，能够在一定的时间内收集、管理、处理、整理，从而成为网络安全问题的有力工具。而安全态势感知分析技术，则是一种基于大量安全风险的计算方法，能够迅速提高计算机对复杂环境中的威胁特征进行识别、理解、分析、响应和处理等方面的计算手段，将其有机地结合在一起，必然会成为我国网络安全的最佳途径。

参考文献：

[1]毛远军. 基于大数据的网络安全态势感知技术分析[J]. 科学与信息化，2019（5）.

[2]王闪闪. 基于大数据的网络安全态势感知与关键技术分析[J]. 网络安全技术与应用，2022（10）：3.

[3]管磊，胡光俊，王专. 基于大数据的网络安全态势感知技术研究[J]. 信息网络安全，2016（9）：6.

[4]管磊，胡光俊，王专. 基于大数据技术的网络安全态势感知平台研究[J]. 保密科学技术，2016（5）：7.

[5]王以伍，张牧. 基于大数据的网络安全态势感知关键技术研究[J]. 电脑知识与技术：学术版，2020，16（15）：4.

作者简介：蔡波（1984—），男，四川南充人，本科，助教。研究方向：大数据技术、计算机网络及通信技术。

邓飞（1984—），男，四川眉山人，硕士，讲师。研究方向：大数据技术、计算机网络及通信技术。

杨露平（1990—），女，四川广元人，本科，中学二级教师。研究方向：大数据技术、计算机网络及通信技术。